TECHNISCHE UNIVERSITÄT MÜNCHEN

Fakultät für Informatik
Lehrstuhl für Wirtschaftsinformatik
Prof. Dr. Helmut Krcmar

Assessing the Information Security Status of an Organization from a Management Perspective

Rainer Diesch

Vollständiger Abdruck der von der Fakultät für Informatik der Technischen Universität München zur Erlangung des akademischen Grades eines

Doktors der Naturwissenschaften
(Dr. rer. nat.)

genehmigten Dissertation.

Vorsitzende:	Prof. Dr. Claudia Eckert
Prüfer der Dissertation:	1. Prof. Dr. Helmut Krcmar
	2. Prof. Dr. Jens Grossklags

Die Dissertation wurde am 11.01.2021 bei der Technischen Universität München eingereicht und durch die Fakultät für Informatik am 02.07.2021 angenommen.

Preface

Information security has already accompanied me in my previous work experience and during my studies. The freedom to study one topic extensively and to put this research into practice led me to become a doctoral student. This thesis was influenced by numerous people and inspiring persons who I all want to thank.

This work would not have been possible without the support of my doctoral supervisor Prof. Dr. Helmut Krcmar. I want to thank you for the inspiring conversations, discussions about the topic, the possibility of speaking with practitioners, the great support of the whole network of the Chair of Information System (I17) of the Technical University of Munich, and much more. My sincere thanks for your support and guidance.

The work has greatly benefited from the community of the Chair of Information Systems (I17) and the team at the fortiss research institute I had the honor to work with. I want to thank especially Dr. Matthias Pfaff, Dr. Andreas Reidt, Markus Jakob, and Alejandro Arreola Gonzalez which who have accompanied the way from the beginning.

This work further profited from great scholars and practitioners I was privileged to discuss my papers and the results of my work with. Thank you all for your support, the critiques, inspiring ideas, and true feedback.

Finally, I want to thank my parents, my brothers, and my girlfriend Myriam. Your unconditional love and support made this work possible. Thank you very much!

Munich, Germany, 18.12.2020 Rainer Diesch

Abstract

Problem Statement: Despite a growing body of knowledge in the research area of information security and especially in information security assessment, organizations struggle in quantifying their information security status in order to make decisions on a management level. Therefore, this thesis addresses the following challenges regarding information security assessment from a management perspective: (1) missing comprehensive view on information security, (2) available metrics do not meet management requirements, (3) missing link between technical metrics and management objectives, and (4) missing comprehensive information security assessment standard. The thesis develops a conceptual information security assessment dashboard to contribute to a possible solution of the described challenges.

Research Approach: The research approach follows the design science paradigm with three iterations to develop the results. In respect to this approach, multiple methodologies were used for data gathering (literature search, semi-structured expert interviews, focus groups), data analysis (literature analysis, open-axial-selective coding, qualitative content analysis), artifact development (Goal-Question-Metric approach, information security metrics aggregation method), and evaluation (semi-structured expert interviews, focus groups, simulation, informed argument).

Results: This thesis provides several empirical findings within the three iterations of the design science methodology. Starting with a review of available literature to distinguish terms that are often used as synonyms, identify research streams, and propose a research agenda in the field of information security assessment to introduce the problem. Following the research agenda, (1) the thesis suggests 12 factors that influence information security management decisions and their interrelations to generate a comprehensive model. The development of (2) a methodology to aggregate information security metrics in accordance with management needs combined with a review of existing information security metrics leads to the (3) development of a conceptual information security assessment dashboard from a management perspective.

Contributions: The thesis provides several contributions to theory and practice. The delimitation of terms and the method of information security factors that influence decision-makers extend the knowledge of information security within organizations, the underlying aspects, and interdependencies. The thesis presents a new way of aggregating information security metrics by meeting the needs of management. It also contributes to research in the field of information security assessment and helps practitioners with existing metrics to present them to the management. The dashboard itself provides a comprehensive, comparable, traceable, actionable, and useful view on an organization's information security status and contributes to theory by showing a way to reduce negative effects on decision-quality explained by the decision theory such as information overload, information asymmetry, and information aggregation.

Study Limitations: The results of this thesis are subject to limitations. The evaluation of the results is based on semi-structured expert interviews and focus groups and covers only a small number of organizations and industries with a focus on large organizations. Therefore, the results may be limited in generalizability. Despite the different measures to reduce validity and reliability issues, not all results are tested with quantitative experiments and studies and therefore could be biased by subject meanings of interviewees or the researcher's judgement.

Future Research: Based on the findings and limitations, this thesis opens several possibilities for future research. This includes the (1) quantitative evaluation and extension of the suggested comprehensive model of information security factors, (2) the usage of the information security aggregation methodology to develop further measuring tools, and (3) the implementation of the conceptual information security assessment dashboard to test the performance by making decisions. Also, (4) the comparison of the information security status of different organizations and (5) tool-based recommender systems for decision-support.

Table of Contents

List of Figures

List of Tables

List of Listings

List of Appendices

List of Abbreviations

SJR	Scimago Journal & Country Rank
IS	Information Security
ICT	Information and Communication Technology Security
CS	Cyber Security
CR	Cyber Resilience
MSF	Management Success Factor
CIA	Confidentiality, Integrity and Availability
CEO	Chief Executive Officer
CIO	Chief Information Officer
CSO	Chief Security Officer
ISMS	Information Security Management System
CISO	Chief Information Security Officer
ISO	Information Security Officer
BCM	Business Continuity Management
ROSI	Return on Security Investment
GQM	Goal-Question-Metric
KPI	Key Performance Indicator
CMDB	Configuration Management Database
ISF	Information Security Forum
C	Challenge
RQ	Research Question
CVSS	Common Vulnerability Scoring System
DSR	Design Science Research
DSRM	Design Science Research Methodology

List of Symbols

∩	Intersection
∪	Union
Σ	Summation
%	Percentage
\	Set difference
Ø	Average

Part A

Introduction to the Thesis

1 Introduction

"The term information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability." (Office of the Law Revision Counsel, 2007)

Information security rises in importance and value over the past years. The global market value of information security increased from $88 billion in 2012 to $145 billion in 2018 (Australian Cyber Security Growth Network Ltd., 2019). The report of the Australian Cyber Security Growth Network Ltd. (2019) also predicts that the global market value is set to increase by 86% to $270 billion from the last actual data of $145 billion until 2026. This growth rate not only shows the importance of information security for the global market but also for organizations and their business models.

Business models and services are based or even fully dependent on data (Knapp et al., 2006). Information security is necessary for organizations to protect their information and consequently their business models. If an organization fails to address information security, the probability of an incident is significantly increased. Security breaches not just cause financial losses for organizations but also legal and reputation repercussions (Tu/Yuan, 2014). The financial damage of a data breach ($3.86 million on average (Ponemon Institute LLC, 2018)) without law and reputation consequences is often too high for organizations to survive. This is not only important for large organizations. According to Thycopic Software Ltd. (2017), 62% of all cyber-attacks are hitting small- and mid-sized businesses. 60% of these are going out of businesses six months after such an attack. This shows that attacks mostly do not target specific organizations. The reasons for the attacks also show the insignificance of organization size. 25% of breaches were intended to gain strategic advantages (espionage) while 71% were financially motivated (Verizon Communications Inc., 2019). These attacks are valuable for the attackers considering that enormous sums are paid for vulnerabilities. For example, the organization Zerodium constantly increases its payouts for vulnerabilities up to $2.5 million in 2020 (Zerodium, 2020).

1.1 Problem Statement

Information security has long been the responsibility of technical employees (Willison/Backhouse, 2006). While getting more and more important, information security gains business-attention (Ransbotham/Mitra, 2009) and also the responsibilities shifted from technical employees to the management. Information security managers, today, are fully responsible for information security issues and must take them into account in the organization (Abu-Musa, 2010; Soomro/Shah/Ahmed, 2016). An example, which even demands this duty in writing, is the German Stock Corporation Act (§91 section 2) that requires active risk management. This law points out that in the absence of an effective contractual provision, the member of the executive board has unlimited liability with his private assets (§93 section 2 and §43 section 2). However, information security and business managers are not necessarily information security experts. Therefore, different standards and best practices were developed to guide through managing information security and continuously improve the information security status of an organization. Standards such as the ISO/IEC 27000 series (ISO/IEC, 2018) or COBIT (ISACA, 2012) deal with the management and governance perspective of information security within organizations. Others such as the NIST 800 series (NIST, 2008) or the Standard of Good Practices from the Information Security Forum (ISF) (ISF, 2018), deal more with technical aspects to protect information. Research in the past also focusses on information security management with different tasks and their effectiveness. Soomro/Shah/Ahmed (2016) conducted a systematic literature review on the topic of information security management and revealed the following research areas: “Overall management role”, “Information systems security policy making”, “Human factor/HRM”, “Information systems security as a board level issue”, “Information systems security awareness and compliance training”, “Top management support”, “Integration of technical and managerial activities”, “Information systems security as a business issue”, “Business IT/IS alignment”, “Information architecture”, “Information systems security risk assessment”, and “Cloud computing and security management issues”. Both, research and practice, suggest the information security assessment as a major part of information security management within organizations to continuously improve the information security status of an organization.

“If you can’t measure it, you can’t improve it.” (Peter Drucker)

The quote of Peter Drucker shows this in extreme. It means that you can not be successful unless you can define and constantly track success. Managers must be able to consider technical threats as well as other factors mentioned above to take the right and effective measures to mitigate threats. (Coronado et al., 2009). To provide necessary funds, make good decisions and argue to the business, information security managers must understand the complexity of information security (Willison/Backhouse, 2006) and have a comprehensive view of the topic (Soomro/Shah/Ahmed, 2016). To address this challenge, standards and best practices provide metrics for information security. Also, research deals with metrics development (Collier et al., 2016; Young et al., 2016), taxonomies (Vaughn/Henning/Siraj, 2003; Pendleton et al., 2017), individual metrics with their performance (Boyer/McQueen, 2007; Holm/Afridi, 2015), and metrics visualization (Savola, 2007).

There is a growing number of industry reports and academic studies available that describe different parts of information security assessment. However, large information security incidents and data breaches are being reported more and more frequently in the daily news. To avoid these issues, an organization has to know how secure their information systems are, at any given point in time (Mermigas/Patsakis/Pirounias, 2013). Due to the complex topic of information security within organizations and the constant reporting on information security issues, it can be argued that the knowledge about information security assessment is limited. The following Challenges (Cs) were identified, that have not been addressed in the literature yet:

C1 Missing comprehensive view on information security. Information security remains a major challenge for organizations (Soomro/Shah/Ahmed, 2016). The different areas of information security such as awareness, physical security, infrastructure, or vulnerabilities combined with the different information security management tasks described above make information security a complex construct within organizations (Willison/Backhouse, 2006). Standards and best practices explain the implementation of an Information Security Management System (ISMS) and support information security managers. However, these standards and best practices are very generic in scope and tend to be abstract (Siponen/Willison, 2009). These standards also consist of a huge amount of information. The amount of information with different focus areas also shows the complexity of information security, but in practice leads to a fall back to ad-hoc implementations. Therefore, Mijnhardt/Baars/Spruit (2016) asks for an easy to understand toolkit. Current literature focusses on factors that influence information security separately. Examples are organizational factors (Kankanhalli et al., 2003; Narain Singh/Gupta/Ojha, 2014), policy compliance (Höne/Eloff, 2002; Goel/Chengalur-Smith, 2010; Johnston et al., 2016), or human factors (Gonzalez/Sawicka, 2002; Kraemer/Carayon/Clem, 2009; Alavi/Islam/Mouratidis, 2016). A comprehensive view on existing information security factors that influence decision-making is asked by various researchers (Soomro/Shah/Ahmed, 2016; Horne/Maynard/Ahmad, 2017) and would help to understand the complexity of information security within organizations.

C2 Available metrics do not meet management requirements. Information security metrics are a common method to assess the information security status of an organization. A McKinsey study shows that management reports lack in *structure*, *clarity*, and *consistent real-time data* (Boehm et al., 2018). The lack of *structure* is due to the high amount of information with too-high levels of detail within management reports. These reports are overloaded with technical acronyms and are not made to get an easy overview from a management perspective. Therefore, the reports are not *clear* and understandable for managers. The lack of *consistent real-time data* leads to conflicting reports of different divisions of an organization in which the context of the given metrics is not clear. Comparability of metrics with different contexts, the derivation of measures, and the understanding of the current information security status can not be done with existing information security reports. Information security metrics within reports and their development is in an early stage and quite underdeveloped (Savola, 2009; Zalewski et al., 2014). Therefore, the knowledge of how to measure the defense level of organizations and generally of systems is a gap in research (Vaughn/Henning/Siraj, 2003; Purboyo/Rahardjo/Kuspriyanto, 2011; Alavi/Islam/Mouratidis, 2016).

C3 Missing link between technical metrics and management objectives. Information security metrics can be classified by their measurement objective. Vaughn/Henning/Siraj (2003) developed an information assurance metrics taxonomy that shows different measurement areas of metrics. *Program developmental metrics* measure if an organization has chosen policies and processes, *support metrics* measure the support for the security programs within organizations such as awareness, *operational metrics* measures the operational information security support, *effectiveness metrics* measure the organizations actually providing defense (Vaughn/Henning/Siraj, 2003). Besides these clusters, Vaughn/Henning/Siraj (2003) also suggest metrics for strength assessment as well as metrics for weakness assessment. This classification is one example to classify and describe existing metrics in the literature. The question remains what the individual metrics measure and what these metrics mean from a management perspective. Savola (2007) stated that security metrics are used for decision support in conjunction with risk management decisions. Further, Savola (2007) concluded that technical, operational, or organizational security management and the metrics will be associated with risk analysis directly or indirectly. However, several authors pointed out the missing link between information security metrics and management goals (Bayuk/Mostashari, 2013; Collier et al., 2016; Pendleton et al., 2017).

C4 Missing comprehensive information security assessment standard. Standards such as ISO/IEC 27004 (ISO/IEC, 2009) or NIST SP 800-55 (NIST, 2008) provide different information security metrics. However, by their own account, they do not cover the minimum information security requirements necessary for organizations (NIST, 2008). Also, the metrics often measure the existence of processes and the effective implementation of countermeasures, but not if the countermeasure is effective (Bayuk, 2013). Because of missing comprehensive metrics and as a consequence of the above-mentioned challenges (C1-C3), information security countermeasures are often implemented “more or less at random” (Boehm et al., 2018) and managers often take decisions based on their experience, judgment and to their best knowledge (Chai/Kim/Rao, 2011). Researchers (Dogaheh, 2010; Maier et al., 2017; Al-Darwish/Choe, 2019; Tewamba et al., 2019) and practitioners (Boehm et al., 2018) pointed out the need for a comprehensive information security dashboard. Consequently, there is no comprehensive information security assessment standard available in the literature.

1.2 Research Goal and Guiding Questions

The aim of this thesis is the development of a conceptual information security assessment dashboard for information security managers of an organization.

This goal tackles the selected research gaps from the challenges described above in the discipline of information security by broadening the understanding of information security assessment. To achieve this goal the following description introduces the guiding Research Questions (RQs) that will be addressed in this thesis:

RQ1: *What are the current challenges regarding information security assessment?*

RQ1 is asked to respond to the existing challenges in the field of information security assessment. To answer the question, three goals are set: (1) The identification, definition, and demarcation of different terms in the field of information security. (2) The thematic classification and identification of research streams within the information security metrics domain. (3) The identification and description of current challenges with results in a research agenda. While answering *RQ1*, a state-of-the-art literature analysis provides a broad overview of the topic and ensures that the challenges are not being solved yet.

RQ2: *Which are the most important information security factors that influence information security management decisions?*

Research describes different factors that might influence information security. To develop a conceptual information security assessment dashboard from a management perspective and addressing the challenge that current metric development approaches are not goal-oriented (Rudolph/Schwarz, 2012), *RQ2* investigates in revealing the most important for them. Answering *RQ2* will not only require the suggestion of information security management factors but also its interdependencies and thus a comprehensive view of information security decision making by organizations from a management perspective.

RQ3: *Which metrics are suitable for quantifying aspects of the information security management factors?*

The definition of information security metrics is still at an early stage of research, and the literature has shown inconsistency in providing suitable metrics for assessing information security. To broaden the current understanding of metrics, what they measure, what they mean, and which metrics are useful for quantifying aspects of information security management factors, a consolidation of existing metrics and a classification based on the results of these metrics would be helpful.

RQ4: *How can information security metrics be prepared for the information security management of an organization?*

Speier-Pero (2019) points out that aggregated information presented to managers do have an impact on decision-making quality while information overload, on the other hand, leads to the use of heuristics for decision-making and the reduction of confidence in the decision. To prepare technical information security metrics from *RQ3*, this Research Question focuses on the development of an information security metrics aggregation method that reduces the described drawbacks from existing aggregation methods.

RQ5: *How can a comprehensive dashboard for information security assessment be designed to meet management needs?*

RQ5 is asked to achieve the overall goal of this thesis. Dashboards are requested from research and practice to overcome the given challenges mentioned above. To answer this question, the information security metrics aggregation method of *RQ4* is used to develop key indicators for the information security management of an organization. The conceptual dashboard helps information security managers to understand the information security areas, making well-informed decisions, and provide action alternatives for improvement. Researchers can benefit from a comprehensive information security assessment dashboard by testing the metrics in practice, examining the impact of information security decisions, collecting relevant data for other research objectives, and testing a variety of information security theories.

Each RQ and the according publication is related and derived out of the introduced challenges. Table 1.1 illustrates which challenge is tackled by which RQ.

Challenge not addressed in extant literature		RQ1	RQ2	RQ3	RQ4	RQ5
C1:	Missing comprehensive view on information security	●	●			●
C2:	Available metrics do not meet management requirements			●	●	●
C3:	Missing link between technical metrics and management objectives				●	●
C4:	Missing comprehensive information security assessment standard		●	●		●

Notes. C: Challenge; RQ: Research Question; ●: Addresses challenge

Table 1.1: *Mapping of challenges to the addressed research questions*

1.3 Structure

This cumulative thesis is divided into three main parts (Part A: Introduction to the thesis, Part B: Publications, Part C: Summary of Results and Discussion of Implications) as illustrated in Figure 1.1 and outlined in the following paragraphs:

Part A : This part begins with the motivation and the problem statement followed by the objective and structure of the thesis (see Chapter 1). The basic theoretical background, the used terms, and an overview of related work are given in Chapter 2. Chapter 3 closes Part A by illustrating the overall research approach and the used methods to achieve the thesis goals.

Part B[1]: The second part of the thesis consists of five peer-reviewed publications (Chapter 4 to Chapter 8). The first publication (see Chapter 4) focuses on current challenges in the information security assessment and metrics domain, the demarcation of terms, and the development of a research agenda. Publications two and three (Chapter 5 and Chapter 6) focus on the one hand on the definition of information security management objectives and the other hand on related metrics that quantify aspects of these objectives. The fourth publication in Chapter 7 supposes a method to aggregate information security metrics. The last publication (see Chapter 8) uses the previous findings in order to develop a conceptual dashboard for information security assessment.

Part C : The last part concludes the thesis. There, a summary of the proposed results of the publications is given (see Chapter 9). Chapter 10 discusses the contributions of the findings to theory and practice. Limitations of the thesis are outlined in Chapter 11. Finally, the thesis closes with recommendations for future research (see Chapter 12).

Publications: The five peer-reviewed publications contributing to the goals of the thesis are embedded in Part B. Each publication is summarized in the following itemization as

[1] Part B consists of Part B1: Published Articles and Part B2: Working Papers (WP).

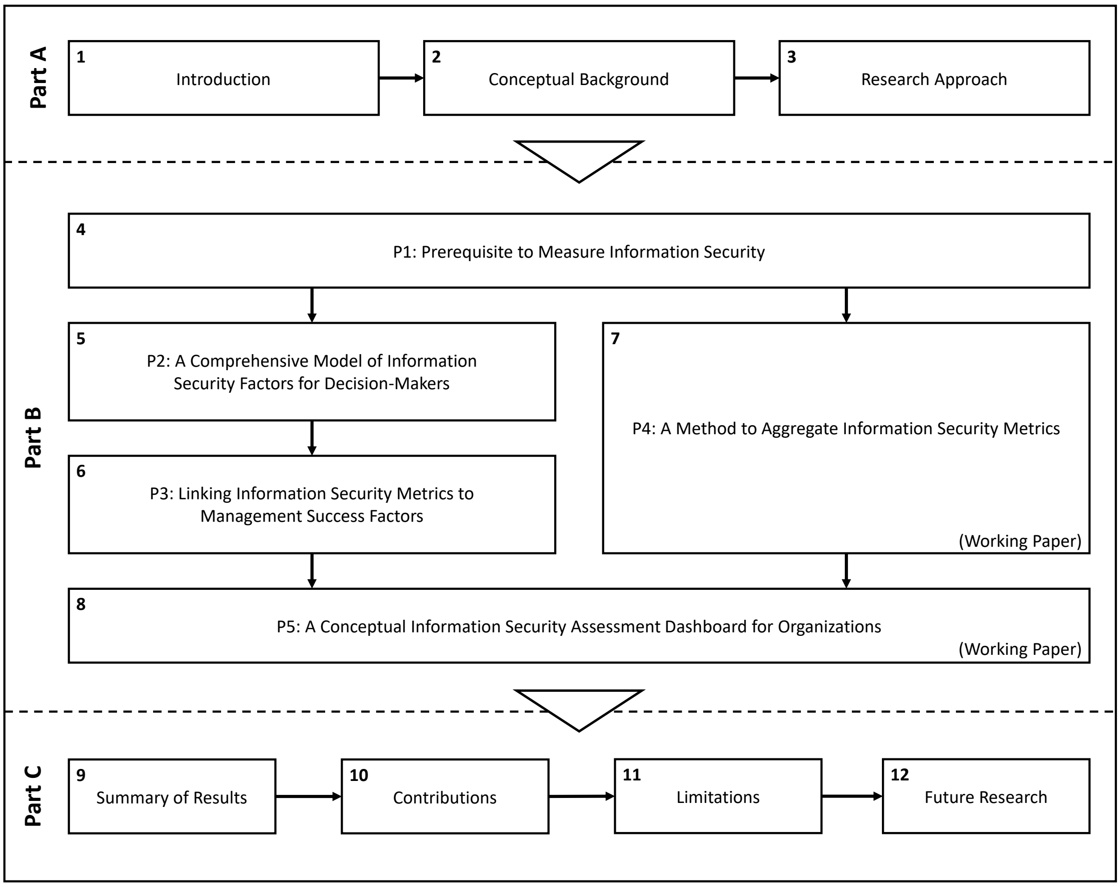
Part A
1
Introduction
2
Conceptual Background
3
Research Approach
Part B
4
P1: Prerequisite to Measure Information Security
5
P2: A Comprehensive Model of Information Security Factors for Decision-Makers
6
P3: Linking Information Security Metrics to Management Success Factors
7
P4: A Method to Aggregate Information Security Metrics
(Working Paper)
8
P5: A Conceptual Information Security Assessment Dashboard for Organizations
(Working Paper)
Part C
9
Summary of Results
10
Contributions
11
Limitations
12
Future Research

Figure 1.1: *Structure of the thesis*

illustrated in Figure 1.1. For each publication the research problem, the methodological approach, and the main contributions are briefly outlined:

P1: Prerequisite to Measure Information Security. Information security measurement and therefore metrics are an important instrument for information security assessment. However, information security metrics development and research are in a very early stage (Savola/Heinonen, 2011; Zalewski et al., 2014) and current research asks for intensified research in measuring and monitoring information security-related data (D'Arcy/Herath, 2011; Fenz et al., 2014; Sommestad et al., 2014). Therefore, this study provides a state-of-the-art literature review according to Webster/Watson (2002) to give an overview of current research attempts in the field. The study provides three main contributions: (1) The delimitation of the terms Information Security (IS), Information and Communication Technology Security (ICT), Cyber Security (CS), and Cyber Resilience (CR). (2) A classification of current literature with the related research streams "Security management", "Security measurement", "Human behavior", and "Practical frameworks". (3) Possibilities for future research for each of the discovered streams related to the measurement of information security.

P2: A Comprehensive Model of Information Security Factors for Decision-Makers. Information security within organizations is a complex phenomenon. The understanding of this complex topic is necessary for information security managers to provide necessary funds, make good decisions, and argue to the business management (Willison/Backhouse, 2006). However, a comprehensive view with specific factors and their interdependencies related to information security decision-making is not available in the existing literature (Kraemer/Carayon/Clem, 2009; Soomro/Shah/Ahmed, 2016; Horne/Maynard/Ahmad, 2017). This study combines a literature search according to Webster/Watson (2002) with an open-axial-selective coding (Corbin/Strauss, 1990) to analyze the literature followed by a semi-structured expert interview with information security managers to provide the first comprehensive model of Management Success Factors (MSFs) for information security decision-makers.

P3: Linking Information Security Metrics to Management Success Factors. Information security metrics are a common method to assess the information security status of an organization. Various metrics are described and discussed according to their performance in research articles (Premaratne et al., 2008; Dogaheh, 2010; Holm/Afridi, 2015). Also, practical frameworks, standards, and best practices such as the ISO/IEC 27004 (ISO/IEC, 2009) or the NIST SP 800-55r1 (NIST, 2008) supposes different information security metrics. However, these metrics are not goal-oriented (Bayuk/Mostashari, 2013; Pendleton et al., 2017; Azuwa/Sahib/Shamsuddin, 2017) and do not meet management requirements. Therefore, this study uses a state-of-the-art literature analysis (Webster/Watson, 2002) in conjunction with the Goal-Question-Metric (GQM) approach (Basili/Weiss, 1984) to develop a mapping between existing information security metrics and the information security management success factors.

P4: A Method to Aggregate Security Metrics. Information security metrics in practice tend to be technical and are computed to key indicators for information security managers. The problems of these computed indicators and metrics from a management perspective are: (1) too many metrics available, (2) not goal-oriented, (3) not quantifiable, (4) not comparable, (5) not comprehensible, and (6) not actionable. By using a design-science approach (Hevner et al., 2004) in combination with a simulation and a semi-structured expert interview to evaluate the results, this study proposes an information security metrics aggregation method to overcome these problems.

P5: A Conceptual Information Security Assessment Dashboard for Organizations. The assessment of information security is important not only for large companies but also for small and medium-sized enterprises. People responsible for information security are not necessarily information security experts. Especially in small- and medium-sized enterprises, there is the need for an easy to understand and comprehensive view on the information security status of the organization. However, a standard for measuring information security is not yet available (Alshaikh et al., 2014; Arabsorkhi/Ghaffari, 2018; M'manga et al., 2019), but the need for information security dashboards is present (Dogaheh, 2010; Al-Darwish/Choe, 2019; Tewamba et al., 2019). Therefore, this study provides a conceptual information security assessment dashboard based on the previous suggested results **(P1-P4)**, the design-science methodology (Hevner et al., 2004), and the evaluation with experts from a leading global organization.

The following Table 1.2 summarizes the publications that are embedded in this thesis in Part B, providing information on the authors, title, outlet, type, and rank for each publication.

No.	Authors	Title	Outlet	Type	Rank
P1	Diesch, Pfaff, Krcmar	Prerequisite to Measure Information Security - A State of the Art Literature Review	ICISSP 2018 (published)	CON	h5 Index[2]: 12
P2	Diesch, Pfaff, Krcmar	A comprehensive model of information security factors for decision-makers	C&S (published)	JNL	ERA[3]: B
P3	Diesch, Krcmar	SoK: Linking Information Security Metrics to Management Success Factors	ARES 2020 (published)	CON	CORE[4]: C
P4	Diesch, Pfaff, Krcmar	Reducing Complexity - A Method to Aggregate Security Metrics	C&S (submitted)	JNL	ERA: B
P5	Diesch, Krcmar	A Conceptual Information Security Assessment Dashboard for Organizations	JMIS (submitted)	JNL	VHB[5]: A

Notes. P: Paper; ICISSP: International Conference on Information Systems Security and Privacy; CON: Conference; C&S: Computers & Security; JNL: Journal; SoK: Systematization of Knowledge; ARES: International Conference on Availability, Reliability and Security; JMIS: Journal of Management Information Systems

Table 1.2: *Summary of embedded publications*

[2] Google's h5 Index 2020, http://scholar.google.de

[3] http://portal.core.edu.au/jnl-ranks/365/

[4] http://portal.core.edu.au/conf-ranks/923

[5] https://vhbonline.org/vhb4you/vhb-jourqual/vhb-jourqual-3/gesamtliste

2 Conceptual Background

Information security assessment has the purpose to deliver information to information security managers in order to derive actions, make decisions, and further improve the information security status of an organization. Therefore, the basis of this thesis is mainly influenced by two fields of research. First, Section 2.1 introduces the field of information security with basic concepts and definitions, an introduction to information security management, and current research and practice of information security assessment. The second field of research is dealing with management and decision-making as a prerequisite and a consequence of information security assessment. Decision theory with behavioral decision-making as well as information and their effects on decision-quality is introduced in Section 2.2.

2.1 Information Security

Information security has its origins at the beginning of hierarchical command and control structures in administration and warfare (de Leeuw et al., 2007). Cryptography was the first attempt to protect information and dates back to 1900 BC, and the hieroglyphic symbols documented the story of a lord's life. (Kahn, 1997). Further techniques to encrypt and protect information were for example the Cipher Disk, the Vigenère-Cipher, and the Saint-Cyr-Slide. These techniques are made by hand but built the basis of modern information security by providing possibilities to protect information. The rise of the extensive literature in the field of information society does, however, not deal with security issues. The first substantial contribution in the sub-area of cryptography came from Kahn (1967) with the book *Codebreakers* (de Leeuw et al., 2007).

With the rise of computers and networks, computer security started to become important. 1961, Vyssotsky and McIlroy developed a game for IBM, in which computer programs tried to destroy each other (de Leeuw et al., 2007). After seen security as a "by-product of correctness" (de Leeuw et al., 2007), several viruses and worms were present in the 1990s which lead to the development of firewalls and the serious start of today's information security. Information security is defined variously in the literature and does not only contain the limitation of technical systems. The ISO/IEC (2018) defines information security as the "preservation of confidentiality, integrity, and availability of information". One other definition that is more technical comes from Whitman/Mattord (2012) which defines information security as "the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information". For this thesis, the general definition of the Office of the Law Revision Counsel (2007) is used:

> *"The term information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability." (Office of the Law Revision Counsel, 2007)*

The terms security and safety are often used together and also as synonyms in the literature. The difference between security and safety is illustrated by Schneier (2003) which stated that “security is about prevention” while safety is “protecting assets from unintentional actions”. In this context, unintentional actions are caused by the internal functions of a system itself. In other words: A safe system does not accept any unintended states while a secure system is a safe system that does just accept states which do not lead to unauthorized information access or modification (Eckert, 2013).

This thesis builds on the basic concepts of information security, information security management, and information security assessment. Therefore, the following subsection outlines the basic concepts and defines the different terms used in this thesis.

2.1.1 Basic Concepts and Definitions

Distinction of different synonyms of information security

Past literature uses different terms to describe information security without considering their differences. Information and Communication Technology Security (ICT), Information Security (IS), Cyber Security (CS), and Cyber Resilience (CR) are often used as synonyms but are not the same. For this thesis, the following definitions of the different terms based on Diesch/Pfaff/Krcmar (2018) are used and illustrated in Figure 2.1.

- “ICT is the protection of information which is stored or transmitted via a technical system”. The often-used terms “IT security” and “systems security” in literature is subsumed under ICT.
- “IS [...] is the protection of information which can be stored or transmitted without using technical systems.” Therefore, this term includes the research area of security awareness.
- “CS [...] describes the protection of assets without any information but with a relationship to them.”
- “CR is not just about the protection of assets but also to ensure business delivery despite adverse cyber events.”

Protection goals

As defined above, information security is about measures which provide integrity, confidentiality and availability. The following itemization introduces the properties briefly:

- *Integrity* is the “property of accuracy and completeness” (ISO/IEC, 2018). The protection includes measures against unauthorized modifications or deletion of information. This property is not only important in order to protect stored information but also during the transportation of information. If an attacker modifies, replaces, or deletes messages during transportation, integrity is violated.

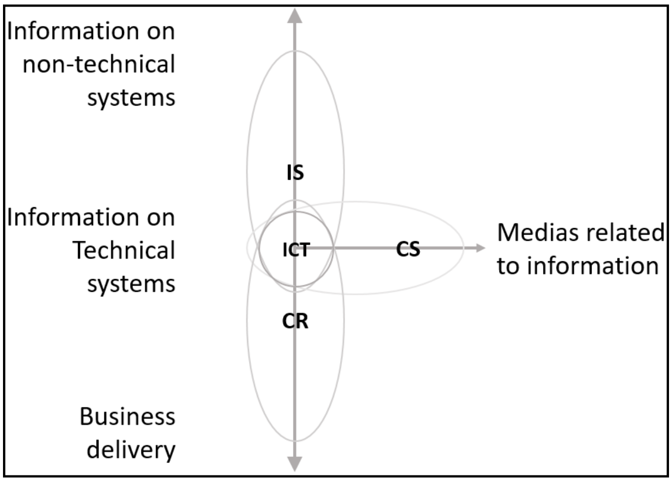
Information on non-technical systems
Information on Technical systems
Business delivery
IS
ICT
CS
CR
Medias related to information

Figure 2.1: *Overview of different terms (Diesch/Pfaff/Krcmar, 2018)*

- *Confidentiality* is defined as the “property that information is not made available or disclosed to unauthorized individuals, entities, or processes” (ISO/IEC, 2018). This definition includes not only attackers as an individual but also entities and processes. The confidentiality is violated if an attacker gets unauthorized access to information for example by eavesdropping.

- The *availability* is the “property of being accessible and usable on demand by an authorized entity” (ISO/IEC, 2018). In other words: If an authenticated and authorized subject has the ability and the right to access information, the subject can not be compromised in accessing the information.

In addition to these properties, further goals can be added. The ISO/IEC 27000 (ISO/IEC, 2018) includes optional properties such as authenticity, accountability, non-repudiation, and reliability. The focus of this thesis is on information security assessment from the management perspective and therefore at the level where the initial objectives are sufficient.

Information security breach

Information security breaches occur when compromising specific assets of an organization. To ensure information security, measures have to be implemented within a defined scope that is to be protected. In practice, risks are used as a tool to prioritize and scope measures. Risks also explain how information security breaches emerge and what the prerequisites for a breach are. A risk is generally defined as an “effect of uncertainty on objectives” (ISO/IEC, 2018). A risk of a information security threat is further characterised as the probability of occurrence combined with the potential consequences (damage) (Eckert, 2013). A risk is only present if an asset with a specific value has a vulnerability and a threat potential combined with a probability of compromise. Yeh/ Chang (2007) described that “risk occurs when assets are vulnerable to threats”. The following itemization gives a brief definition of the used terms while the interrelations between them are illustrated in Figure 2.2.

- *Assets* are goods of an organization worthy to protect or "anything that has value to the organization" (ISO/IEC, 2005).
- *Threats* have the goal to exploit vulnerabilities or weaknesses to violate confidentiality, availability, or integrity of an asset (Eckert, 2013).
- A *weakness* is a weak point of an asset that potentially could be a vulnerability while a *vulnerability* is a weak point that can be used in order to bypass, deceive, or modify the security services of an asset unauthorized (Eckert, 2013). A vulnerability is a weakness that can be exploited by a threat.

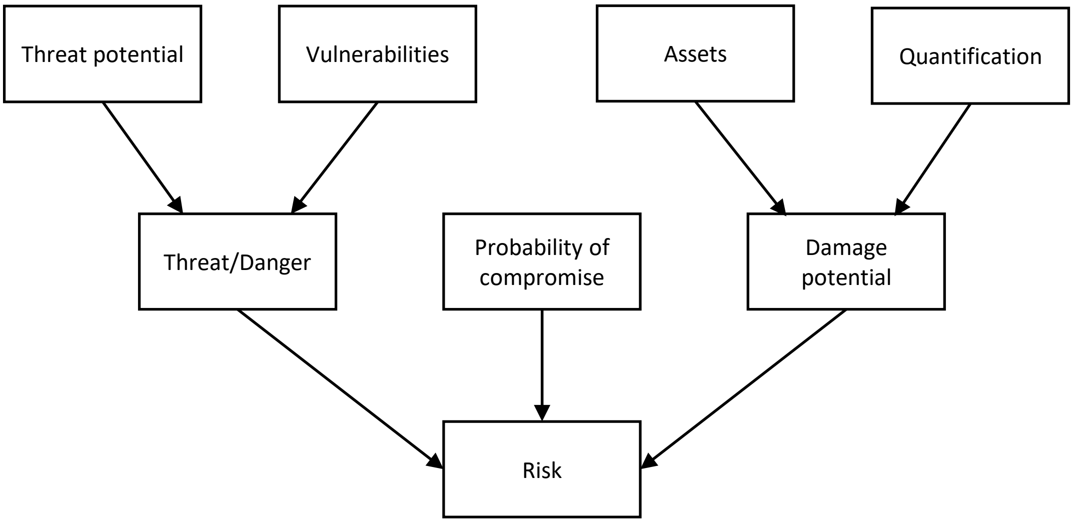

Figure 2.2: *Relationship between threats, vulnerabilities, and risks (based on Eckert, 2013)*

2.1.2 Information Security Management

On the one hand, managers are leading persons of an organization. On the other hand, the management of an organization is about the "control of business activities in order to provide for continuous improvement in the performance of that activity in order to achieve organisational objectives" (Ashenden, 2008). One main challenge of management is the configuration of resources. To decide rigorously, management systems - a "set of interrelated or interacting elements of an organization to establish policies and objectives and processes to achieve the objectives" (ISO/IEC, 2018) - have to be implemented by organizations.

An Information Security Management System (ISMS) is defined as "that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security" (ISO/IEC, 2005). The main objective of information security risk management is to avoid threats or reduce their impact under attack (Yeh/Chang, 2007). The definition of an ISMS includes the different tasks necessary for information security management. To support organizations, different standards and best practices are available to help organizations to establish an ISMS. The most popular standard is the ISO/IEC 27000 series that introduces minimum requirements for establishing an ISMS. These standards are used in practice "to ensure consistent, repeatable, and auditable means of addressing Information Security issues" (Ashenden, 2008).

An essential component of information security management as defined above is risk management. Figure 2.3 illustrates the components of a risk management process that includes all activities to systematically deal with information security risks. Risk identification has the goal to systematically capture existing risks regarding information security in order to potentially violate business processes. The risk analysis is about a qualitative and quantitative evaluation of the risks. In this activity, risks are computed based on the previously described characteristics possibility of compromise and impact. The risk control is about the decision of how to handle existing risks. There, the economic perspective in the form of cost-benefit analysis has to be considered. The costs are the measures to reduce the risk and the benefit would be the increase in the information security status. The effectiveness of measures is computed and reported within the last step. This step also includes measures that try to identify risks that are not identified in the first step. (Krcmar, 2015)

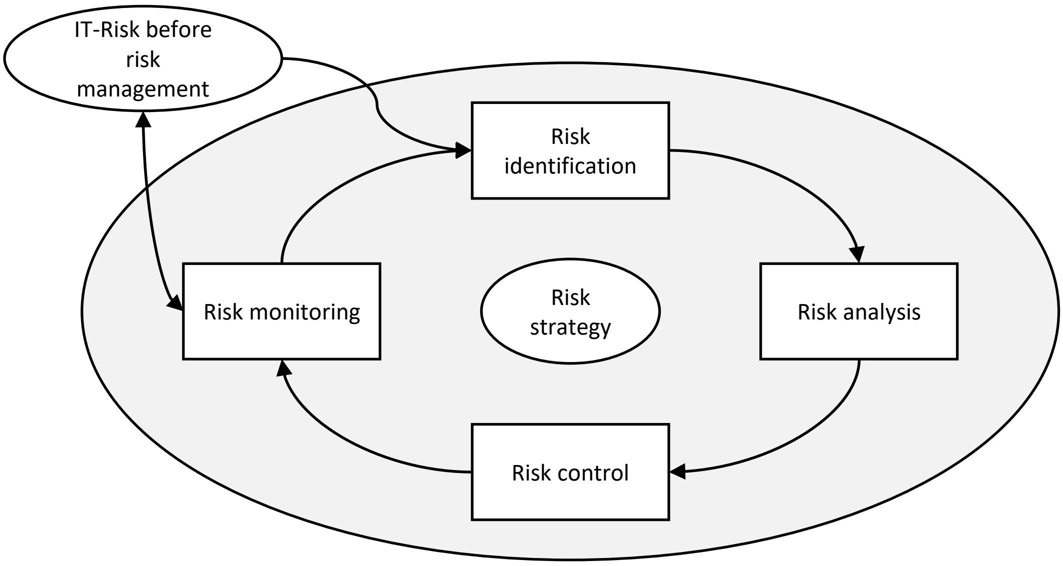

Figure 2.3: *Risk management process (based on Krcmar, 2015)*

Silic/Back (2014) conducted a literature review about information security and give an overview of previous research in the field of information security. Research in the past focus on "risk assessment", "privacy", "information security governance", "asset management", "human resources security", "physical and environmental security", "communications and operations management", "access control", "information systems acquisition, development and maintenance", "information security incident management", "business continuity management", "compliance", and "Economics". Two years later, Soomro/ Shah/Ahmed (2016) published a literature review about information security management. This research suggests similar areas but related to management practices: "overall management role", "security policy making", "human factor/HRM", "security as a board level issue", "security awareness and compliance training", "top management support", "integration of technical and managerial activities", "security as a business issue", "business IT/IS alignment", "information architecture", "security risk assessment", and "cloud computing and security management issues". These two literature reviews show that most of the areas are very similar. The difference is the focus on information security in general, which includes areas such as privacy and economics while the more specific information security management areas include more specific topics that are suggested as problems for information security management.

As described above, risk management and especially the included risk assessment is a major task of information security management in research and practice. The knowledge of the current information security level of an organization is not just important to measure the effectiveness of measures but also to define management goals and analyze as well as monitor risks. The following subsection gives an overview of existing concepts from practice and findings from research on the area of information security assessment.

2.1.3 Information Security Assessment

Risk assessment deals with the identification, analysis, management, estimation, and evaluation of possible risks within an organization (Silic/Back, 2014). Silic/Back (2014) and Soomro/Shah/Ahmed (2016) identified the major findings of research within this research area as summarized in Table 2.1. The purpose of information security management is to establish and provide a predefined level of security suitable for a specific organization. The reduction of risks through measures should lead to an increase in the security level. A major challenge and a difficult task is the quantification of an information security status (Mermigas/Patsakis/Pirounias, 2013; Tu/Yuan, 2014; Krcmar, 2015; Horne/Maynard/Ahmad, 2017).

Category	Finding	Original author
Risk identification	How to identify and deal with risks in the early development phases.	(Boehm, 1991)
Risk analysis	A method to identify and quantify software development risks.	(Barki/Rivard/Talbot, 1993)
Risk control	Risks can be reduced more effectively if managers are aware of the full range of controls available to them.	(Straub/Welke, 1998)
Risk monitoring	A spacial (risk-driven) approach for software development.	(Boehm, 1988)

Table 2.1: *Summary of past key findings of risk management (based on Silic/Back, 2014)*

While literature focuses on risk assessments, information security assessment methods and thus the quantification of the information security status of an organization is rarely present in past literature. Soomro/Shah/Ahmed (2016) revealed studies that use (1) quantitative approaches based on the risk definition with the quantification of risk exposure, the probability, and the expected loss (Bodin/Gordon/Loeb, 2008), (2) qualitative approaches based on experts' estimated potential loss (Feng/Li, 2011), and (3) the combination of quantitative and qualitative approaches (Zang, 2014). Soomro/Shah/

Ahmed (2016) concluded that holistic approaches for information security assessment are necessary for decision-making, but are missing in the literature.

Information security assessment can be performed not only based on a risk approach, but also on a control-based approach. Standards and best practices such as the ISO/IEC 27000 or the NIST SP 800-53 (NIST, 2013a) provide documents with recommended controls for organizations. Audits and assessments are then based on these controls to evaluate the organizations' compliance. The challenge of this approach is the consideration of the complex relationships between all information security concepts which leads to unsuitable approaches and decreases organizations' performance (Fenz et al., 2013). Organizations "need to distinguish between controls they need and those that are less critical" (Tu/Yuan, 2014).

A common method to assess aspects of the information security status of an organization and continuously monitor risks are metrics. In literature, a common sense is that metrics are the basis for decisions and therefore, should be well-understood (Bayuk, 2011) and should help distinguish between needed and less critical controls. Terms in the context of information security measures, metrics, and measurements are constantly used in different contexts and meanings. Therefore, the following terms are used for this thesis:

- *Measure* and *countermeasure* are used as synonyms for "protective measures [...] prescribed to meet the security requirements" (Jafari et al., 2010). This definition is in conjunction with "improving the overall information security state by selecting the best security countermeasures (controls) to protect their information assets" (Yulianto/Lim/Soewito, 2016).

- *Measurement* is the "process to determine a value" (ISO/IEC, 2018). In other words, the process of estimating attributes of an object (Pendleton et al., 2017).

- *Metric* refer to "assigning a value to an object" (Pendleton et al., 2017). A more precise definition with the same meaning is that metrics are "elements that provide quantitative data on different aspects that can be useful to evaluate the effectiveness of a security control" (Herrera, 2005).

- *Indicators* are "combinations of the data provided by the metrics, so that they provides useful information to the organization" (Herrera, 2005).

Security metrics are well present in standards and best practices as suggestions for information security managers and technical employees. The ISO/IEC 27004 (ISO/IEC, 2009), NIST 800-55 (NIST, 2008), Information Security Forum (ISF) (ISF, 2018), or the Common Criteria (CCIB, 2017) are just a few of them. The described metrics, however, do not cover the minimum information security requirements (NIST, 2008) and measure the compliance of these standards rather than addressing security (Bayuk, 2013). The literature review of Diesch/Pfaff/Krcmar (2018) identified "metrics development", "metric taxonomies", "separate security metrics", "effectiveness", and "metrics visualization" as existing research streams in literature. Table 2.2 illustrate the major streams with a description and example findings.

Stream	Description	Examples
Metrics development	Methods to develop information security metrics.	• Goal-Question-Metric approach (Basili/Weiss, 1984) • Attack-graphs (Idika/Bhargava, 2012)
Metric taxonomies	Description of different metrics and measurement characteristics.	• Types of metrics and metrics in different contexts such as operations, program development, or effectiveness (Vaughn/Henning/Siraj, 2003) • Metrics on different abstraction levels and classification based on their input type. (Purboyo/Rahardjo/Kuspriyanto, 2011)
Separate security metrics	Individual metrics are developed and evaluated for efficiency or effectiveness.	• The mean time to compromise and VEA-bility score (Premaratne et al., 2008) • The Common Vulnerability Scoring System (CVSS) (Holm/Afridi, 2015)
Effectiveness	Metrics and constructs which influence information security effectiveness.	• Propose a model of five factors influence information security effectiveness without evaluation or data collection (Coronado et al., 2009) • Model of factors describing metrics quality (Savola, 2013)
Visualization	Visualizing metrics and indicators in an understandable way.	• Requirements for information security visualization (Savola/Heinonen, 2011)

Table 2.2: *Research streams in the field of security metrics (based on Diesch/Pfaff/Krcmar, 2018)*

2.2 Decision Theory

Information security assessment is used in order to provide a basis for decision-making. Therefore, decision theory has an impact and should be considered when developing models or other theories of information security assessment.

Decision theory has its origins in 1936-37 where the term "operational research" first appears and "the problem of how decision are or ought" are discussed. These early contributions lead to the assumption that decision making can be studied scientifically which leads to several fundamental contributions such as linear programming, decision and game theory. This leads to the formal description of decision problems with mathematical and logical models (Tsoukiàs, 2008).

Besides the axioms of von Neumann/Morgenstern (1944) (also known as the utility function), Etner/Jeleva/Tallon (2012) said that one of the major achievements of decision theory is considered to be the work of Savage (1954). von Neumann/Morgenstern (1944) formulated axioms that explain: If a decision-maker is faced with different choices the optimal decision will be the one that maximizes the expected value of the utility derived from the choice. The core axiom of Savage (1954) explains that when comparing two decisions, it is "not necessary to consider states of nature in which these decisions yield the same outcome" (Etner/Jeleva/Tallon, 2012). Since then, different research directions appear. One of them was based on management science because a major task of managers is to make decisions (Koontz, 1980). The definition of Polasky et al. (2011) is used for this thesis:

> *Decision theory is "a powerful tool for providing advice on which management alternative is optimal given the available information" (Polasky* et al.*, 2011).*

2.2.1 Behavioral Decision Theory

Each decision is made under uncertainty. This uncertainty is represented by the set of possible states of a system with a dedicated probability of occurrence (Koontz, 1980). Already in the 1960s the observation of decisions within complex organizations shows a gap between real decisions within complex organizations and rational behavior, which is explained by decision theory. (see Cyert/March, 1963).

The behavioral decision theory deals with the different decision-making heuristics used in practice and how they perform in contrast to rational decision-making (Csaszar/Eggers, 2013). Two major research streams are available within behavioral decision theory. (1) Managing is about how people work and therefore includes interpersonal relationships, individual psychology, motivations, leadership, and experience. (2) Group behavior influence decisions which include sociology, anthropology, and social psychology (Koontz, 1980).

Csaszar/Eggers (2013) also summarized a major finding of behavioral decision theory that explains that heuristics can perform in a similar matter than optimal decision rules under certain conditions. The biggest influence on decision-quality derives from uncertainty. This uncertainty is represented by different concepts such as data asymmetry, aggregation, or availability that influence decisions in practice. The relevant concepts are explained in the following section.

2.2.2 Information and their Influence on Decision-Quality

Information has received great attention from researchers of different areas such as information in organizations, decision-making, decision-making behavior, and virtual environments because of the importance of information in different decision-making situations (Afzal/Roland/Al-Squri, 2009). This leads to the concepts of information asymmetry, information overload, and information aggregation.

Information asymmetry

Information asymmetry describes the imbalance of available information between different groups. In contrast: Information symmetry is when all relevant information is present to all parties involved (Afzal/Roland/Al-Squri, 2009). Past research studied information asymmetry in the context of transactions when a seller has more information than a buyer (Akerlof, 1970). In this context, multiple studies deal with the imbalance between the information available to buyers and sellers and how they value different products based on the information available (see Afzal/Roland/Al-Squri, 2009).

Information asymmetry is not only important if different groups are involved but also within organizations or group members. The imbalance of information between group members can affect decisions because the members have an influence on these decisions according to the behavioral decision theory. For example, an increase in information asymmetry leads to an increase in a group member's manipulative tendency and the effectiveness of this manipulation (Malekovic/Sutanto/Goutas, 2016).

Information asymmetry is the imbalance of information between different groups or group members.

Information overload

Information overload is defined as the phenomenon of having too much information to process them as a human. Butcher (1995) categorized three main areas of research within management science according to information overload:

1. **The problem of personal information overload:** Researchers study aspects of this problem deal for example with questions on how information overload affects a manager's ability to manage or how information overload can be managed personally. The main concerns are personal faxes, emails, or computer-generated reports.
2. **The problem of organizational information overload:** Information overload within organizations is seen as a major issue caused by too much paper and too much electronic information.
3. **The problem of customer information overload:** This problem is related to the effects of information overload on customers' spendings.

The ability to process information is dependent on the environmental load with information and explained by Driver/Mock (1975). Increasing information load results in an increase of the ability to process information, to the point where the information processing capacity of decision-makers decreases. This phenomenon is the effect of "information overload". Decision-quality, in this case, is positively related to information processing (Hwang/Lin, 1999). Figure 2.4 illustrates the described relationship.

Information overload describes if there is "more information available than necessary for processing a task and where this extraneous information has a detrimental effect on decision quality" (Speier-Pero, 2019).

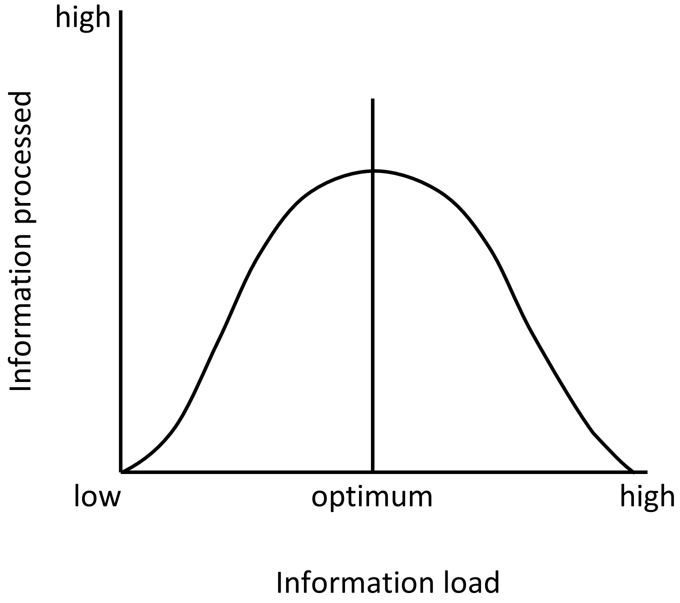

Figure 2.4: *Relationship between information processing and information overload (based on Driver/Mock, 1975)*

Information aggregation

Information aggregation in the context of management decisions is not as present in the literature as information asymmetry and information overload. It might be the case, that if information aggregation is done to a certain degree, information underload is a result and indirectly included within the description of information overload. Nevertheless, information aggregation is studied in the context of presenting information to management and provide decision support. To not present hundreds of data points, these are often aggregated. An example would be a financial report. Speier-Pero (2019) summarized the existing literature, which indicates that detailed data lead to more accurate decisions.

Information aggregation is the "combination of information according to some type of integration rules" (Speier-Pero, 2019) and thus a reduction of available information.

3 Research Approach

The aim of this thesis is the development of a conceptual information security assessment dashboard for information security managers of an organization. The field of design science "attempts to create things that serve human purposes" (March/Smith, 1995). This definition fits the purpose of this thesis by instantiating the definition: (1) create things - conceptual dashboard; (2) information security manager - human; (3) information security assessment - purpose.

The following Section 3.1 includes a detailed description of the research strategy used to develop the conceptual dashboard. Section 3.2 describes the research methods in detail used to generate the results.

3.1 Research Strategy

As mentioned above, this thesis is based on the Design Science Research (DSR) paradigm conceptualized by March/Smith (1995). The research framework of March/Smith (1995) is technology-oriented and distinguishes between the research outputs construct, model, method, and instantiation. Built on the work of March/Smith (1995), Hevner et al. (2004) introduces a framework and guidelines to conduct, evaluate, and present DSR in the information systems domain. DSR within this thesis is understood as follows:

> *"Design science [...] creates and evaluates IT artifacts intended to solve identified organizational problems" (Hevner* et al.*, 2004). An IT artifact includes products, processes, constructs, design principles, models, methods, technological rules, and instantiations (Gregor/Hevner, 2013).*

Hevner et al. (2004) has not explicitly described a process to develop a design science research artifact. Therefore, this thesis adopts the DSRM for information systems research introduced by Peffers et al. (2007). The DSRM consists of a process with six core activities to develop an artifact in accordance with the guidelines of Hevner et al. (2004). The following enumeration describes the activities of the process briefly:

1. **Problem identification and motivation:** This action involves the description of the research problem that is later used for the development of a solution. Also, the value of a possible solution should be outlined in order to: (1) motivate the researcher and the audience, (2) increase the acceptance of the results, and (3) increase the understanding of the reasoning behind the researcher's thoughts and association of the problem.

2. **Define the objectives for a solution:** This action includes a detailed description of the objectives that should be inferred from the problem definition in accordance with what is possible and feasible.

3. **Design and development:** This action is about the creation of the artifact. “Conceptually, a design research artifact can be any designed object in which a research contribution is embedded in the design” (Peffers et al., 2007).

4. **Demonstration:** The goal of this step is to show how the artifact solves one or more instances of a problem. This demonstration can be done using the artifact in a real-world scenario or with the use of methods such as experimentation, simulation, case study, or others.

5. **Evaluation:** This activity has the main goal to measure and observe how well the artifact supports a solution to the described problem. The evaluation is dependent on the nature of the problem and can be performed in various ways. “Conceptually, such evaluation could include any appropriate empirical evidence or logical proof” (Peffers et al., 2007). Hevner et al. (2004) also suggests rigorous methods such as case/field study, simulation, or informed argument to evaluate an artifact appropriately.

6. **Communication:** The last activity involves the presentation of the problem and its importance, the artifact, its utility and novelty, the rigor of its design, and its effectiveness to the relevant audience such as researchers or practitioners. This is typically done by publishing academic articles or by involving practitioners in the process.

DSR is “inherently an iterative and incremental activity” (Hevner et al., 2004). Also the process of Peffers et al. (2007) provides feedback loops from the evaluation or the communication back to the design or the definition of objectives. A design artefact is considered to be complete if it satisfies the requirements and solves the problems that was meant to solve (Hevner et al., 2004).

Concerning the DSRM, Chapter 3 and 2 as well as the first publication (P1) introduce and motivate the problem according to the first step of the DSRM. To develop the conceptual dashboard, three iterations of the DSRM were made in order to solve the guiding Research Question (RQ) (sub-problems) and propose the result after the third iteration. The results of the three iterations are as follows:

1. A conceptual model of information security factors for decision-makers (P2).

2. A method to aggregate security metrics (P4).

3. The conceptual information security assessment dashboard from a management perspective (P3, P5).

Table 3.1 shows the included publications of this thesis with their iteration number, the phases of the DSRM done within them as well as the used methods to gather information, develop, demonstrate, or evaluate the artifacts. The methods are explained in more detail in the following Section 3.2.

	DSRM activity						
P/C/I	**1**	**2**	**3**	**4**	**5**	**6**	**Methods used**
P1/4/-	•					•	- Literature review
P2/5/I1	•	•	•	•	•	•	- Literature review - Open-axial-selective coding - Semi-structured expert interview - Qualitative content analysis
P3/6/I3	•	•	•			•	- Literature review - Open-axial-selective coding - Goal-Question-Metric approach
P4/7/I2	•	•	•	•	•	•	- Simulation - Informed argument - Semi-structured expert interview - Qualitative content analysis
P5/8/I3	•	•	•	•	•	•	- Information security metrics aggregation method - Workshop/Focus group - Qualitative content analysis

Notes. P: Paper; C: Chapter of the thesis; •: DSRM process addressed in publication; I: DSR iteration number

Table 3.1: *Publications with methods and the relation to the DSRM*

3.2 Research Methods

Literature review

A literature review "seeks to describe, summarize, evaluate, clarify, and/or integrate the content of primary reports" (Cooper, 1988) and is "essential for any academic project" (Webster/Watson, 2002). A literature review helps researchers to understand the body of knowledge, provide a solid theoretical foundation, substantiate the presence of research problems, argue the novelty of the own research, and framing the valid research methodologies, approach, goal, and research questions (Levy/J. Ellis, 2006). The challenge of literature reviews in information systems are (1) the interdisciplinary nature of topics and (2) the structuring of these reviews. To overcome these challenges, (Webster/ Watson, 2002) recommended guidelines to conduct and structure a systematic literature review. Relevant steps for conducting a literature analysis recommended by Webster/ Watson (2002) are:

- *Identify relevant literature:* The three-step approach of Webster/Watson (2002) to identify relevant literature starts with a keyword search within relevant outlets. The recommendation is to start with leading journals in the field with selective relevant conference proceedings. The quality of a literature review lies mainly on the selection of databases, outlets (i.e. journals, conferences, or books), and keywords (vom Brocke et al., 2009). Second, the references within the identified publications of the keyword search should be reviewed. This backward-search ensures the consideration of previous relevant publications. The third step is to use tools that capture which articles cite the article identified in steps one and two. This process includes the refinement of relevant sources, keywords, and databases and is considered to be completed if no more new concepts appear in the publication set.

- *Structuring the review:* The relevant literature identified should be analyzed according to the specific goal of the review. Webster/Watson (2002) differentiate between an author-centric and a concept-centric approach to structure the publications. The author-centric approach assigns the different concepts to the respective author. A concept-centric approach lists the concepts and shows the respective authors aligned to them. The natural process of reviewing the literature is author-centric because the relevant publications are analyzed by its concepts. But, the author-centric approach rather fails to synthesize past literature (Webster/Watson, 2002). Therefore, a concept-centric approach should be preferred.

The literature review is used several times within this thesis, but with different objectives. Each publication in Part B starts with a literature review in order to provide a foundation and argue the novelty of the research. A synthesis of past research with the development of a research agenda is the objective of the first included publication within this thesis (Chapter 4). The proposed three-step approach to identify relevant literature was also used in combination with the open-axial-selective coding instead of the concept-analysis. The open-axial-selective coding is recommended as a rigorous method to analyze literature (Wolfswinkel/Furtmueller/Wilderom, 2013) and has the advantage of analyzing the whole context of a publication and not extracting abstract concepts.

Open-axial-selective coding

Grounded theory is about "how the discovery of theory from data - systematically obtained and analyzed [...] - can be furthered" (Glaser/Strauss, 1967).

A grounded theory not only describes but also explains phenomenons. It is a method to discover theory from data systematically obtained. The data for grounded theory can come from various sources such as interviews, observations, government documents, video tapes, newspapers, letters, or books - "anything that may shed light on questions under study" (Corbin/Strauss, 1990). Literature in the past evolves different procedures for data collection and analysis. Corbin/Strauss (1990) explained 11 canons and procedures used in conjunction with grounded theory. The authors also explained the three basic coding types of the grounded theory approach - the open-axial-selective coding. This coding is the "fundamental analytic process used by the researcher" to analyze data in grounded theory and is relevant for this thesis:

1. *Open coding:* The first step of coding is about the identification and labeling of concepts within the data. It is an interpretive process to break through standard

ways of thinking. Further, the categories are compared with others for similarities and differences as well as grouped together to former categories and subcategories.

2. *Axial coding:* This coding step involves testing the relationship between categories and subcategories against the data. Further categories are developed during this coding step. In particular, subcategories are linked to categories.

3. *Selective coding:* All categories are unified around a “core” category. Also, categories that needs further explanations are filled in with descriptive details. This core category represents the central phenomenon and builds the theory.

Within this thesis, open-axial-selective coding is used to build a theory based on existing literature. Wolfswinkel/Furtmueller/Wilderom (2013) considered this approach as a valid method to analyze also literature out of a literature analysis to concentrate on the whole context of publications and not only their basic concepts as described in the literature review paragraph. A core objective of this thesis is built on open-axial-coding and proposes a theory to describe factors that have an influence on information security managers’ decisions and their interdependencies.

Semi-structured expert interview

Expert interviews can be a method of qualitative empirical research to explore expert knowledge (Meuser/Nagel, 2009). Therefore, expert interviews are a method to gather empirical data as a basis for further analysis. Expert interviews can be characterized based on standardization (structured, semi-structured, not structured), the authority of the interviewer (soft, neutral, hard), type of contact (personally, phone, written), number of interviewers (single, group, survey), and function (investigating and mediating) (Bortz/Döring, 1995). The differentiation of interviews is mainly done by the degree of standardization. A fully standardized (structured) interview consists of predefined questions that are not flexible in wording or order for the interviewer. Within a not structured interview, thematic boundaries are given but the interview is “open” - “it is left to the skills of the interviewer” (Bortz/Döring, 1995).

The semi-structured approach to explore experts’ knowledge is recommended by Meuser/Nagel (2009) to ensure the comparability of different interviews but give enough room for extended explanations when relevant. In semi-structured expert interviews, the results are dependent on the interview guide, the expertise of the interviewees, and the analysis of the information:

1. *Operationalization:* The operationalization is about the development of questions that guide through the interview as well as the possibility to “measure” the intended objective. The construction of an interview guide has a macro- and micro-planning stage (Bortz/Döring, 1995). The micro-planning is based on the research questions and identifies thematic areas of interest considering relevant literature. The macro-planning is about the creation of an interview guide with the order of the thematic areas. The development of an interview guide is an art in its own which aims to neither under- nor overburden the interviewee (Bortz/Döring, 1995).

2. *Expert selection:* An expert is defined by (Bogner/Menz, 2009) as "a person who disposes of, or is believed to dispose of, particular competences, and who consequently has a social status, or exercises a function, which places him/her in a position where he or she may be able to gain general acceptance for his or her action orientations and situation definitions".

3. *Data analysis:* The data analysis is focused on thematic units which are passages with similar topics (Meuser/Nagel, 2009). The qualitative content analysis introduced by Mayring (2015) is a method to analyze material that comes from some form of communication. Because the qualitative content analysis is not only used to analyze the semi-structured expert interviews but also for analyzing the workshop/focus group, this method is described separately within this section.

Using expert interviews was suggested by Sonnenberg/Vom Brocke (2012) as an appropriate method to evaluate the understandability, clarity, and usefulness of design artifacts. This thesis also uses expert interviews in order to evaluate the proposed results of the embedded publications P2 and P4 (see Chapter 5 and 7).

Focus group/Workshop

> *"Focus group methodology is a way of collecting qualitative data, which - essentially - involves engaging a small number of people in an informal group discussion (or discussions) 'focused' around a particular topic or set of issues" (Wilkinson, 2004).*

Expert interviews as described in the paragraph "Semi-structured expert interview" can also be characterized by the number of interviewees (Bortz/Döring, 1995). Based on the definition of focus groups, it can be argued that a focus group is a special form of a group interview. According to Onwuegbuzie et al. (2009), a focus group should last between one and two hours and consist of 6 to 12 participants. A focus group has to be moderated. The moderator is responsible for taking notes, present the focus group a series of questions, give stimulus material, and ask them to respond.

The analysis of a focus group is considered the same as the analysis of data from one-to-one interviews (Wilkinson, 2004). Possible analysis types are constant comparison (grounded theory), classical content analysis, keywords-in-context, and discourse analysis (Onwuegbuzie et al., 2009).

This thesis uses a focus group as an evaluation method for the conceptual information security assessment dashboard. The evaluation of an artifact from design-science with a focus group was recommended by Sonnenberg/Vom Brocke (2012). The analysis was done with the help of a qualitative content analysis described in the next paragraph.

Qualitative content analysis

The list of definitions of qualitative content analysis is long. Mayring (2015) gave six examples of them and concluded six points that characterize qualitative content analysis in common and are understood by this thesis. Qualitative content analysis has the aim to (1) analyze communication, (2) analyze fixed communication, (3) proceed systematically, (4) proceed rule-based, (5) proceed theory-driven, and (6) draw conclusions on certain aspects of communication.

Mayring (2015) describes different methods and processes to analyze content concerning objectivity, reliability, and validity of the outcomes. First, the prerequisite to ensure a "fixed communication", all interviews and communications have to be transcribed into text. After that, Mayring (2015) introduces different "analysis-techniques" suitable for different types of research questions. In the following, the relevant techniques for this thesis namely *summarizing content analysis*, *valence or intensity analysis*, and *contingency or interrelation analysis*.

The *summarizing content analysis* consists of three steps:

1. **Paraphrasing.** This step contains the deletion of text areas with no contribution to the research objective or text areas with little content. Also, a standardized level of language and a grammatical short form has to be produced.

2. **Generalization.** This step takes the paraphrases and prepares them on an abstract level. Predicates are generalized in an equal form and theoretical assumptions are made in case of doubt.

3. **Reduction.** The reduction step generates the overall summary of opinions and thus contributes to the research question. There, phrases with the same meaning are deleted, phrases of similar meanings are combined, very content-bearing phrases are selected and theoretical assumptions are made in case of doubt. This step can be done multiple times.

To analyze quantitative aspects or interdependencies, the *valence or intensity analysis (V)* and *contingency or interrelation analysis (I)* are proposed by Mayring (2015) and used as follows for this thesis:

1. Formulate a question to analyze the material.

2. Determine the material sample.

3. Define the variables (V) / text modules for interrelation (I).

4. Define the scale (V) / rules for interrelation (I).

5. Coding of the material based on the variables and scales.

6. Analyze the codes by their number of occurrence (V) or joint appearance (I).

7. Presentation and interpretation.

Goal-Question-Metric approach

The GQM approach was supposed by Basili/Weiss (1984) in the software engineering domain. The original purpose was to prevent errors in software systems. The GQM was developed in order to provide metrics that (1) are focused on specific goals, (2) can be applied to all life-cycle products, processes and resources, and (3) can be interpreted based on characterization and understanding of the organizational context, environment, and goals (Basili/Caldiera/Rombach, 1994). The method is based on the following three steps:

1. The definition of an objective with respect to models of quality related to a particular environment. This could be resources that are items used by processes to generate an outcome. The purpose of measurement is set by specifying the goal.
2. The characterization of the way the assessment of a specific goal is going to be performed. Questions are developed to characterize the object of measurement with respect to the goal. The goal is refined in characterizing questions.
3. For every question, a set of metrics (data) is associated. These metrics are answering the previously defined question quantitatively. The questions are answered in refining them to metrics.

Simulation

> *"A simulation is an imitation of the behaviour of a real-world process or system over time" Johannesson/Perjons* (2014).

The reproduction or prediction of the behavior of a system can be simulated based on computer simulations. Even complex simulations such as climate change or strategic management can be simulated (Johannesson/Perjons, 2014). Simulations in conjunction with the design-science approach are useful to show the behavior of the artifact (demonstration) or evaluate it (evaluation) by "execute the artifact with artificial data" (Hevner et al., 2004). Simulations are done to reduce the disadvantages of the experimentation with a real system. These might be high costs, time-consuming experiments, the control of the experimental conditions, or if the real system does not exist (Robinson, 2004).

Robinson (2004) reviewed several simulation processes and proposes four steps to conduct a simulation study:

1. *Conceptual model:* The development of a conceptual model requires the recognition of a real-world problem. Within this step it is determined whether a simulation is suitable or not. To develop an understanding of the problem, preliminary or contextual data is used. This data also serves to identify the data required for the computer model.

2. *Computer model:* The process of model coding converts the conceptual model into a computer model. Computer simulation tools and own programming are examples of how this step can be accomplished.

3. *Solutions/understanding:* The computer model serves as the object of experiments to gain a better understanding of the real world. Also, a search for solutions to real-world problems is possible. The three key-issues within this step are (1) “obtain sufficiently accurate results”, (2) “searching within the solution space”, and (3) “testing the robustness of the solution” (Robinson, 2004).

4. *Real world:* This step is the implementation in the real world. This could be the implementation of a solution, the model itself, or the communication of the improved understanding.

Informed argument

The method of informed argument is proposed by Hevner et al. (2004) and Johannesson/ Perjons (2014) as a rigorous method to evaluate artifacts of design-science research. The informed argument method “use information from the knowledge base [...] to build a convincing argument for the artifact’s utility” (Hevner et al., 2004). The argumentation is about the evaluation if an artifact fulfils the defined requirements and can solve the explicit problem by reasoning and arguing. This form of evaluation is rather weak because it could “easily be biased by the background and interests of the researcher” (Johannesson/ Perjons, 2014). Therefore, informed argument is always combined with other evaluation methods within this thesis.

Part B1

Published Articles[*]

[*] In this part, the original publications are slightly modified, including the unification of format and reference styles, the correction of spelling errors, and minor orthographic and grammatical revisions. Furthermore, the references included in each research study have been integrated and are presented at the end of this dissertation. The published version of the included publications can be found in the Appendix.

4 Prerequisite to Measure Information Security

Title	Prerequisite to Measure Information Security - A State of the Art Literature Review
Authors	Diesch, Rainer^{1,2} (diesch@fortiss.org) Pfaff, Matthias^{1,2} (pfaff@fortiss.org) Krcmar, Helmut^{2} (helmut.krcmar@tum.de) ^{1}fortiss GmbH, Guerickestraße 25, 80805 Munich, Germany ^{2}Technical University of Munich (TUM), Boltzmannstraße 3, 85748 Garching, Germany
Type	Conference and Proceedings
Outlet	Proceedings of the 4th International Conference on Information Systems Security and Privacy 2018; Editors: Paolo Mori, Steven Furnell, Olivier Camp; ISBN: 978-989-758-282-0
Publisher	SCITEPRESS[3]
Ranking	h5 Index[4]: 12
Status	Published
How to Cite	Diesch, R.; Pfaff, M. and Krcmar, H. (2018). Prerequisite to Measure Information Security - A State of the Art Literature Review. In Proceedings of the 4th International Conference on Information Systems Security and Privacy - Volume 1: ICISSP, ISBN: 978-989-758-282-0, pages 207-215, doi: 10.5220/0006545602070215.
Individual Contribution	Conceptualization, Methodology, Investigation, Data Curation, Writing - Original Draft, Writing - Review & Editing, Visualization

Table 4.1: *Bibliographic details for P1*

[3] https://www.scitepress.org/

[4] Google's h5 Index 2020, http://scholar.google.de

Prerequisite to Measure Information Security - A State of the Art Literature Review

Abstract: The field of information security is growing in research and practice over the past years. Recent studies highlight a gap in measuring and monitoring information security. In this context various definitions and synonymous expressions exist to describe information security. The aim of the work is to compare and delimit the various terms in this field of research and give a thematic overview of current articles in place. In particular, five dimensions of information security are developed and outlined. Additionally, an overview of possible research directions in the field of measuring and monitoring information security is provided.

4.1 Introduction

The interest in aspects of information security has increased significantly in recent years. There are technical, behavioral, managerial, philosophical and organizational aspects which address the protection of assets and mitigation of threats (Crossler et al., 2013). These aspects are not to be ignored for organizations since these can lead to great harm in case of disregard. Frizell (2015) reported a damage of $15m within one-quarter for Sony Pictures because of a security breach. This cost only included the direct costs of cleaning up the systems. The damage caused by the loss of reputation and other factors were not included. In 2016, the ransomware "wannacry" infected thousands of computers in more than 150 countries. The damage was not only economically as people like patients were affected as their appointments were canceled based on system errors (Bentkower, 2017). Organizations are not just affected because of potential economic damage but also of legal requirements like the security-law in Germany (Bundesanzeiger, 2015).

Recent literature reviews on information security pointed out the need for intensified research in measuring and monitoring information security related data (D'Arcy/Herath, 2011; Crossler et al., 2013; Fenz et al., 2014; Sommestad et al., 2014). This is an obligatory aspect of information security management for making good decisions (Bayuk, 2013). Also, accurate models of the security problem are not in place (D'Arcy/Herath, 2011). A problem which causes a lack of measurement of information security aspects is that the identification of security related data is not well-known (Fenz et al., 2014). But a requirement to collect and measure security related data is to understand the success factors of information security (Sommestad et al., 2014).

The aim of this work is to gain an overview of current research in the field of measuring information security. A state-of-the-art literature analysis is carried out to obtain a comprehensive overview of the area. The goal is not just to show the literature but also to define the different terms in place. Since the understanding is a requirement for measurement, a definition becomes indispensable. Thematic classes of the research area are needed to observe and assign future research.

The paper is organized as follows: Section 4.2 outlines the used method with the scope and the search process to collect relevant literature. Section 4.3 consists of a descriptive analysis, the extracted definitions and thematic classification of the investigated literature. Part 4.4 shows current research challenges for each of the classes. Finally, this work concludes with a conclusion and limitation section.

4.2 Method

To provide a comprehensible literature review, the method of Webster/Watson (2002) and the tool-set of vom Brocke et al. (2009) was used. The specific goals of this review are as follows:

1. Identify, define and delimit different terms in the field of information security.
2. Assign the relevant literature to the definitions and compare it with the used terms of the literature itself.
3. Thematic classification of the literature and show current research gaps.

Search process: Initially, a keyword search is performed within peer-reviewed journals to select high quality articles. Journals from the security field were selected within the Scimago Journal & Country Rank (SJR) with the condition that they are part of the categories security, safety, risk or reliability. Two journals are added because they were used often in the basis literature reviews of (D'Arcy/Herath, 2011; Crossler et al., 2013; Fenz et al., 2014; Sommestad et al., 2014). These are "Computers & Security" and "Information Management & Computer Security". To provide most of the relevant literature the databases ScienceDirect, OpacPlus and Google Scholar were added to the search. As the most relevant literature can be found within the first 100 result of Google Scholar the search was limited to these result set (Silic/Back, 2014). To limit the results the following keyword-string were used (see 4.1).

```
(it OR information OR cyber)
AND (resilience OR security)
AND (factors OR kpi OR measures OR metrics
OR measurement OR indicator OR management)
```

Listing 4.1: *Literature search string*

The first iteration of the search process resulted in a number of hits (Hits[KW]) which are shown in Table 4.2. After that, technical articles and those which are not related to the search topic were excluded based on their title and abstract (Hits[TA]). Finally, articles which described metrics or success factors of information security were marked as relevant. After that, a forward and backward search was carried out to get results which are relevant and were not yet found. The backward search contained all articles which were referenced in the previous iteration and which are of relevance for the information security measurement topic. Google Scholar[1] was used with its function "Cited by" in order to identify all articles which reference the selected one.

[1] http://scholar.google.de

Group	Resource	Hits[KW]	Hits[TA]	Relevant
Information Security	Information Management and Computer Security	99	7	7
	IEEE Transactions on Dependable and Secure Computing	8	1	1
	IEEE Transactions on Information Forensics and Security	7	0	0
	Computers & Security	84	12	9
Databases	Google Scholar	100	11	9
	ScienceDirect	41	6	4
	OpacPlus	110	17	11
Backward			10	10
Forward			24	19
Total		**449**	**88**	**70**

Table 4.2: *Search process matrix*

4.3 Findings

First, a descriptive statistic was done to get a background of the research area. The last row of table 4.2 shows the total amount of articles found in the literature. Only 15.59% of the original articles out of the first search round could be marked as relevant. This leads to the assumption that there are many different phenomena described in the research area. The high amount of articles also assumes the importance and presence in research. Many articles were identified in the forward and backward search (29) within conferences. This can be seen as an indication that the topic is still at the beginning of research. Technically oriented journals just show up with one relevant article. The quantification of information security is therefore mainly part of the security management or related area and not technical-driven.

Since there are many definitions and terms of information security in the literature, the next subsection compares and delimits them. Finally, a classification of the relevant literature in thematic classes are developed to better track and monitor future research.

4.3.1 The Terms in Information Security

A lot of different terms which describe “information security” are in place during the review. These are “Information Systems Security”, “IT Security”, “Information Security”, “Cyber Security” and “Cyber Resilience”.

The basis of the delimitation in this article is the work of von Solms/van Niekerk (2013). They defined three terms in the security area. IS, ICT and CS. The delimitation of the terms is based on the assets which are protected. In this case, ICT is the protection of information which is stored or transmitted via a technical system. “IT Security” or “Systems Security” are defined as synonyms to ICT. IS differs from this because it is the protection of information which can be stored or transmitted without using technical systems. ICT is a part of IS because IS includes the protection of the underlying technology.

CS now describes the protection of assets without any information but with a relationship to them. A bugging operation is an example of this. A technical system (phone) was attacked which has “access” to information which is in human heads. CS is protecting technical systems which have or have no information stored and therefore also includes ICT. CR firstly appears 2013 in form of resilience management Crossler et al. (2013). The only attempt to define CR was done by Björck et al. (2015). They showed 5 dimensions to differ CR from CS. One of these is assets. CR is not just about the protection of assets but also to ensure business delivery despite adverse cyber events. The correlation between the terms is shown in Figure 4.1.

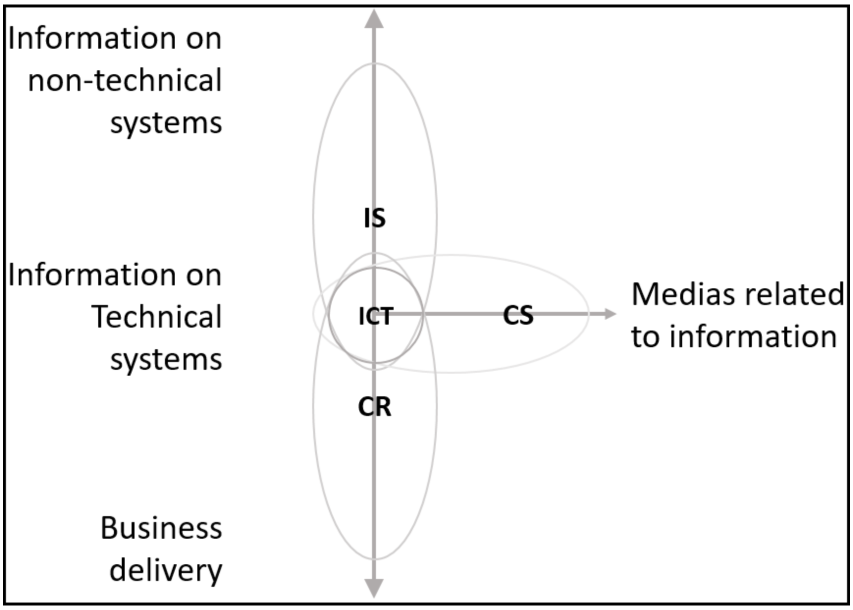
Information on non-technical systems
Information on Technical systems
Business delivery
IS
ICT
CS
CR
Medias related to information

Figure 4.1: *Delimitation of terms*

According to the definition of ICT, IS, CS and CR, the literature was assigned respectively one or more of these in two iterations. First, the article was assigned the term, which the author had intended for this. The basis of the assignment was the terms of the title, abstracts and the keywords. Second, the articles were assigned the terms according to the definition above. This is done based on the context.

The result of the assignment shows that 23 out of 70 articles (32.86%) have the same assignment to the terms for both iterations. It is noticeable that the terms are often used as synonyms. Mainly IS is used as a synonym for ICT. Articles that use the term IS (60) often have just content of ICT included in the text (37) and not IS as defined. All authors used CS and CR as synonyms for ICT. The articles which describe CS or CR used the term IS instead of them. In the present literature, there are clear definitions of the terms, but the terms are not used based on them.

4.3.2 Thematic Classification

The relevant literature of this review is about measurement and metrics of ICT, IS, CS and CR. To observe papers in future and better understand the context, there are several classes produced in this literature review which are based on the keywords of the underlying articles. Each paper is assigned to one of the classes which are shown in Table 4.3.

Security management	Organization and Governance	(Geer/Hoo/Jaquith, 2003; Hong et al., 2003; Trèek, 2003; von Solms/von Solms, 2004; Gupta/Hammond, 2005; Anderson/Moore, 2006; Ernest Chang/Ho, 2006; Johnson/Goetz, 2007; Veiga/Eloff, 2007; Atoum/Otoom/Abu Ali, 2014; Narain Singh/Gupta/Ojha, 2014; Yaokumah, 2014; Fenz et al., 2014; AlHogail, 2015; Horne/Maynard/Ahmad, 2017)
	Awareness	(Straub/Welke, 1998; Velki/Solic/Ocevcic, 2014; Tran et al., 2016)
	Evaluation	(von Solms et al., 1994; Kraemer/Carayon/Clem, 2009; Abu-Musa, 2010; Hall/Sarkani/Mazzuchi, 2011; Norman/Yasin, 2013; Tu/Yuan, 2014; Alqahtani, 2015; Muthukrishnan/Palaniappan, 2016; Azuwa/Sahib/Shamsuddin, 2017)
Security measurement	Development	(Wang/Wulf, 1997; Sharman/Rao/Upadhyaya, 2004; Herrera, 2005; Tanna et al., 2005; Tashi/Ghernaouti-Hélie, 2008; Sowa/Gabriel, 2009; Leon/Saxena, 2010; LeMay et al., 2011; Idika/Bhargava, 2012; Jones/Horowitz, 2012; Tariq, 2012; Bayuk/Mostashari, 2013; Zalewski et al., 2014; Mazur/Ksiezopolski/Kotulski, 2015; Collier et al., 2016; Young et al., 2016)
	Taxonomy	(Vaughn/Henning/Siraj, 2003; Savola, 2007; Savola, 2009; Verendel, 2009; Purboyo/Rahardjo/Kuspriyanto, 2011; Pendleton et al., 2017)
	Security Metrics	(Boyer/McQueen, 2007; Premaratne et al., 2008; Dogaheh, 2010; Jafari et al., 2010; Mermigas/Patsakis/Pirounias, 2013; Holm/Afridi, 2015)
	Effectiveness	(Coronado et al., 2009; Bayuk, 2013; Savola, 2013)
	Visualization	(Savola/Heinonen, 2011)
Human Behavior		(Gonzalez/Sawicka, 2002; Ifinedo, 2012; Crossler et al., 2013; Vance et al., 2014; Montesdioca/Maçada, 2015; Alavi/Islam/Mouratidis, 2016)
Practical Frameworks		(IT Governance Institute, 2007; NIST, 2008; ISO/IEC, 2009; Hayden, 2010; CCIB, 2017)

Table 4.3: *Thematic classification of the literature*

4.3.2.1 Security Management

"Information security management" is used to describe activities for the protection of valuable information assets and mitigate various risks to information coming from all aspects of the organization's environment by applying the security technology and management process (Ernest Chang/Ho, 2006). In other words, it is about processes to control, classify and manage information as well as different guidelines and policies therefrom.

Organization and Governance: These articles deal with organizational processes, policies and their effectiveness. A subset of articles also provides information and simulations of security investments and the security economy within organizations. There are also frameworks on how to set up a secure environment with a culture and guides to good policies included.

Awareness: The role of human in information security is a substantial stream in research (Kraemer/Carayon/Clem, 2009). Therefore organizations have to consider dealing with security awareness.

Evaluation: These articles deal with the question of which success factors lead to good management or which factors influence the success of implementing a security management system. Another aspect is the validation and verification of policies and factors which causes better ones.

4.3.2.2 Security Measurement

Security metrics refer to the interpretation of measurements of the security performance, level and indicators (Savola/Heinonen, 2011). Therefore measurement is the process of estimating attributes of an object while metrics refer to assign a value to an object (Pendleton et al., 2017).

Development: There are methods to develop metrics for information security aspects. Examples of them are metrics which are developed based on different approaches like Goal-Question-Metric (Savola, 2007; Bayuk, 2013) or attack-graphs (Premaratne et al., 2008; LeMay et al., 2011; Idika/Bhargava, 2012). There are also frameworks with descriptions of good metrics and how to implement them.

Taxonomy: The taxonomies in this class describe and characterize different measurement approaches and several classes of metrics which are based on the objective and the measurement goal.

Security Metrics: A security metric is a quantitative indicator for various targets in operational security (Verendel, 2009). The articles focus on specific metrics and evaluate or simulate them.

Effectiveness: The effectiveness of metrics to measure information security is discussed here. The articles compare different frameworks to generate measurements and discuss different metrics in detail.

Visualization: The management has the requirement to easily understand and therefore react very fast to changed metrics (Jafari et al., 2010; Savola/Heinonen, 2011). Therefore these articles deal with an optimal visualization of complex metrics.

4.3.2.3 Human Behavior

Human behavior or human factors affecting information security are not to be confused with the awareness described above. These articles deal with different behavior theories like "protection motivation" or "planned behavior". The perspective of attackers is included in form of social engineering attacks and factors which can prevent them.

4.3.2.4 Practical Frameworks

Frameworks from practice which also called best-practices are included. They are developed for practitioners to deal with information security management systems or security effectiveness.

4.4 Discussion

The quantitative analysis of the relevant literature revealed that under the subject of the measurement of information security many phenomena can be interpreted. An exact delimitation of the topic area from others, such as management processes, would be helpful for tracking this issue. In the case of the definitions, it can be argued that there is less research in CS and CR available than in ICT and IS. Context is the measurement of information security. Future research should pay attention to the correct and uniform use of the concepts and develop them further. The thematic classification shows potential research areas in each of the different classes. The following part describes these research areas within the different classes based on the given literature.

Security Management: To fundamentally make decisions in the area of systems security it is necessary to know the current information security status within an organization and know the weaknesses and where they are. This is currently still a gap in research (von Solms et al., 1994; Johnson/Goetz, 2007; Tu/Yuan, 2014; Horne/Maynard/Ahmad, 2017). Mermigas/Patsakis/Pirounias (2013) goes one step further and says that organizations need to know how secure they are at any given point in time. A requirement to do this is the understanding of the success factors of information security within organizations and how they are related (Kraemer/Carayon/Clem, 2009; Norman/Yasin, 2012; Horne/Maynard/Ahmad, 2017). If the security status can be operationalized it is also possible to measure if the security program as well as their countermeasures or policies of the organization are effective or not. This is also an undeveloped research task (Gupta/Hammond, 2005; Fenz et al., 2014; Atoum/Otoom/Abu Ali, 2014). The present literature review excludes those articles which did not contain any security success factors. Further work could show and categorize the existing direct and indirect success factors which are already in place. This could be the basis for an empirical evaluation and a better understanding of security in organizations.

Security Measurement: The measurement of security as a property and the development of security metrics itself are in a very early research stage and quite underdeveloped (Savola, 2009; Savola/Heinonen, 2011; Zalewski et al., 2014). Knowing how to measure the security as well as the defense level of organizations and generally of systems is a gap in research (Vaughn/Henning/Siraj, 2003; Purboyo/Rahardjo/Kuspriyanto, 2011; Alavi/Islam/Mouratidis, 2016). The area of measurement goes also a step back and asks for practices to measure the coverage of visibility. This is about effective and adequate assessments of risks and assets and how it can be monitored Abu-Musa (2010). Specifically, there is a gap in explored metrics for the measurement of information security, which are associated with existing models and thus provide the basis for cross-sectoral and organizational independent security comparison (Sowa/Gabriel, 2009; Bayuk/Mostashari, 2013). It is often the case that just the security management program is measured and not the security itself (Tashi/Ghernaouti-Hélie, 2008; Jafari et al., 2010). There is not just a gap in developing and creating concrete metrics but also in tools to gather information security related data and monitor the security status (Wang/Wulf, 1997; Boyer/McQueen, 2007; Crossler et al., 2013). Based on this work, current metrics in place could be shown and linked to the frameworks, success factors and development models.

Human Behavior: Human behavior is little represented in this review. In case of measurement there is an open question on how to capture actual behavior (Crossler et al., 2013).

Practical Frameworks: Practical frameworks are designed to help organizations to implement and use security related information in management. The only framework who describes metrics to monitor the security status says that these metrics are not covering the minimum security requirements (NIST, 2008). Also, the automatic way to collect and measure the data is a requirement for good and repeatable metrics (NIST, 2008). Other frameworks like the IT Governance Institute (2007) or ISO/IEC (2009) addresses just the effectiveness of security management processes and not the security status of the assets and environment itself. An empirical evaluation or test of the described issues is not present literature.

4.5 Conclusion

There is a gap in measuring and monitoring information security in current research (D'Arcy/Herath, 2011; Crossler et al., 2013; Fenz et al., 2014; Sommestad et al., 2014). To develop a measurement and collect information security related data, it is necessary to understand information security and the success factors influencing it (Sommestad et al., 2014).

This literature review after Webster/Watson (2002) and vom Brocke et al. (2009) included journals of the information security area as well as databases. The search process results in the identification of 70 articles which are interesting for measuring information security. The chronological analysis shows that the topic has become more and more important in the past years. Also, there are a lot of terms in place which are used in different contexts. This becomes clear as soon as the keywords, the title and the contents of the articles are compared with respect to the term. The delimitation of the terms is based on the work of von Solms/van Niekerk (2013) and is extended in this review based on the definitions of Björck et al. (2015) to get an overview of the current terms and their usage. Past literature uses the terms as synonyms which should be avoided in the future.

The thematic classification of the literature can help to capture future research and better assign them a context. It is shown that the measurement of information security is often a management topic. This is useful because the measurement allows an objective control and a well-based decision-making in connection to information security.

The relevant articles show that information security is necessary for organizations and decision-makers. To manage, make good decisions and capture the current state of information security, a measurement is needed (Bayuk, 2013). Current research does not adequately cover this topic. Future research should investigate in the definition of success factors for information security to fulfill the requirement of understanding security success factors (Kraemer/Carayon/Clem, 2009; Norman/Yasin, 2012; Horne/Maynard/Ahmad, 2017) and define a current state of security (von Solms et al., 1994; Johnson/Goetz, 2007; Mermigas/Patsakis/Pirounias, 2013; Tu/Yuan, 2014; Horne/Maynard/Ahmad, 2017). Therefore concrete metrics and tools to monitor these need to be developed (Wang/Wulf, 1997; Vaughn/Henning/Siraj, 2003; Boyer/McQueen, 2007; Sowa/Gabriel, 2009; Purboyo/Rahardjo/Kuspriyanto, 2011; Crossler et al., 2013; Bayuk/Mostashari, 2013; Alavi/Islam/Mouratidis, 2016). Future research could then evaluate the effectiveness of security programs and actions based on the security quantification (Gupta/Hammond, 2005; Fenz et al., 2014; Atoum/Otoom/Abu Ali, 2014).

4.6 Limitations

The limitations are based on the search process. The initial search was performed based on highly ranked journals. Therefore it is possible that articles within conferences or not included journals could influence the results of this literature review. The same could apply for articles which are excluded based on their title and abstract. It cannot be ruled out that relevant articles have been removed which does not outline to the search topic but has relevant content. In order to limit these shortcomings, the database search, as well as the forward and backward search, was performed. Moreover, this literature review does not cover management or interdisciplinary journals which could also be interesting for measuring security.

5 Information Security Factors for Decision-Makers

Title	A comprehensive model of information security factors for decision-makers
Authors	Diesch, Rainer[1,2] (diesch@fortiss.org) Pfaff, Matthias[1,2] (pfaff@fortiss.org) Krcmar, Helmut[2] (helmut.krcmar@tum.de) [1]fortiss GmbH, Guerickestraße 25, 80805 Munich, Germany [2]Technical University of Munich (TUM), Boltzmannstraße 3, 85748 Garching, Germany
Type	Journal
Outlet	Computers & Security
Publisher	Elsevier Ltd.[3]
Ranking	ERA 2010[4]: B Impact Factor 2018[5]: 3.062 Computers & Security is recommended by the Senior Scholars' Basket of Journals – AIS Special Interest Group Security (SEC)[6]
Status	Published
How to Cite	Diesch, R.; Pfaff, M.; Krcmar, H. (2020): A comprehensive model of information security factors for decision-makers. Computers & Security, Vol. 92, pp. 1–21, doi: 10.1016/j.cose.2020.101747.
Individual Contribution	Conceptualization, Methodology, Formal analysis, Investigation, Data Curation, Writing - Original Draft, Writing - Review & Editing, Visualization

Table 5.1: *Bibliographic details for P2*

[3] https://www.elsevier.com/

[4] http://portal.core.edu.au/jnl-ranks/365/

[5] Clarivate Analytics Journal Citation Reports, https://jcr.clarivate.com/

[6] https://aisnet.org/page/SeniorScholarBasket

A comprehensive model of information security factors for decision-makers

Abstract: Decision-making in the context of organizational information security is highly dependent on various information. For information security managers, not only relevant information has to be clarified but also their interdependencies have to be taken into account. Thus, the purpose of this research is to develop a comprehensive model of relevant MSFs for organizational information security. First, a literature survey with an open-axial-selective analysis of 136 articles was performed to identify factors influencing information security. These factors were categorized into 12 areas: physical security, vulnerability, infrastructure, awareness, access control, risk, resources, organizational factors, CIA, continuity, security management, compliance & policy. Second, an interview series with 19 experts from the industry was used to evaluate the relevance of these factors in practice and explore interdependencies between them. Third, a comprehensive model was developed. The model shows that there are key-security-indicators, which directly impact the security-status of an organization while other indicators are only indirectly connected. Based on these results, information security managers should be aware of direct and indirect MSFs to make appropriate decisions.

5.1 Introduction

Today, most businesses are based or even fully dependent on information such as financial data for banks to stay at the market and be competitive (Knapp et al., 2006). According to Thycopic Software Ltd. (2017), 62% of all cyber-attacks are hitting small- and mid-sized businesses of which 60% are going out of businesses six months after such an attack. 53% of the attacks are causing $500.000 or more (Cisco Systems Inc., 2018) while the average cost of a data breach was $3.86 million (Ponemon Institute LLC, 2018). Not just financial losses are a risk but also legal and reputation repercussions (Tu/Yuan, 2014). Therefore, it is necessary for organizations to keep their information and the underlying technology secure against business-harming attacks.

In the past, information security was purely a technical concern and therefore, technical employees were responsible for information security issues within an organization (Willison/Backhouse, 2006). This perspective fails when it comes to a comprehensive and holistic view and the overall security strategy. Thus, in the past years, there was a shift from the executive technology expert to a management responsibility and a more business-focused view protecting information (Yeh/Chang, 2007; Ashenden, 2008; Ransbotham/Mitra, 2009). Nowadays, security managers are fully responsible to consider and respond to information security issues (Abu-Musa, 2010; Soomro/Shah/Ahmed, 2016). Various cases like the “Equifax breach” had shown the consequences for the top management in case of information security disregards. There, over 146 million personal information were stolen because of an unpatched system, which was a technical shortcoming. This causes, that the company gets rid of their Chief Executive Officer (CEO), Chief Information Officer (CIO), and Chief Security Officer (CSO) by the “retirement” of them right after the breach (Bernard/Cowley, 2017). The technical personal was not affected. This goes further in manifesting the management responsibility within laws like the German Stock

Corporation Act (§91 section 2) which also requires an active risk management within companies.

Because of the shift from a technical to a management perspective, the research focus also changed from studies in a technical context to exploring the management role (Soomro/Shah/Ahmed, 2016). Managers must be able to take technical threats as well as other factors like human behavior into account to take the right and effective actions to mitigate threats (Coronado et al., 2009). To provide necessary funds, make good decisions and argue to the business, it is necessary for information security managers to understand the complexity of information security (Willison/Backhouse, 2006) and have a comprehensive view on the topic (Soomro/Shah/Ahmed, 2016). This comprehensive view with specific factors and their interdependencies as well as the impact on the security status of an organization is still a gap in research (Kraemer/Carayon/Clem, 2009; Norman/Yasin, 2013; Soomro/Shah/Ahmed, 2016; Horne/Maynard/Ahmad, 2017; Diesch/Pfaff/Krcmar, 2018). Therefore, this study has the purpose to identify the key factors, evaluate them and explore interdependencies to finally generate a comprehensive model to understand the information security complexity and thus provide good information security management decisions.

The remaining research article is structured as follows. In Section 5.2, previous work on management practices and Management Success Factors (MSFs) in information security is described and the need for a comprehensive information security model with current shortcomings is shown. In Section 5.3, the three-step methodology which contains the literature survey, the literature analysis, and the expert interview series is presented. In Section 5.4, the evaluated MSFs are provided. The MSFs in conjunction with interdependencies are proposed as a comprehensive model in Section 5.5. In Section 5.6, a critical discussion of the results and areas for future research are highlighted. A conclusion is given in Section 5.7.

5.2 Background and Motivation

This chapter is divided into three sections. In Section 5.2.1, standards and best practices in information security management for practitioners and their shortcomings are described. In Section 5.2.2, the term MSF and the current state of the art in research regarding this topic is introduced. In Section 5.2.3 the need for practitioners, as well as the gap in the literature, are highlighted to motivate this research.

5.2.1 Standards and Best Practices

Information security management is often build based on international standards or best practices (Hedström et al., 2011). The terms "standard" and "best practice" are often used as synonyms but "standards" are usually checked by an international standardization organization while "best practices" and other frameworks are published independently.

The most common standard from such an organization is the ISO/IEC 27000-series (ISO/IEC, 2018). This standard is widely accepted, play an important role and it is possible to certify the organizational information security based on it (Siponen/Willison, 2009). The ISO/IEC 27000-series defines basic requirements in order to implement an information security management system. Also, control guidance, implementation guidance, management measures, and the risk management approach is specified. Special sub-norms are also included in the series, for example, the ISO/IEC 27011 which deals especially with telecommunication organizations.

In addition to the information security management standard, there are frameworks or best practices like the NIST SP800-series (NIST, 2018b), the Standard of Good Practices from the Information Security Forum (ISF) (ISF, 2018) or the COBIT framework (ISACA, 2012). These best practices are used to implement an ISMS, define and develop controls and address the most pressing problems regarding information security with an overview for their risk mitigation strategy (Mijnhardt/Baars/Spruit, 2016). All in all, security standards provide a common basis for organizations to help reducing risks by developing, implementing and measuring security management (Ernest Chang/Ho, 2006).

Information security management certificates do provide a basic assurance level and show that some security measures are available. But in practice, experts are skeptical about certificates. Experts mentioned, that standards do help with compliance but not always help to reduce risk or improve security (Johnson/Goetz, 2007). Lee/Geng/Raghunathan (2016) show, that a higher security standard does not necessarily lead to a higher security level. The following shortcomings of standards were highlighted in the past literature:

(1) Well known standards are very generic in scope and tend to be very abstract (Siponen/Willison, 2009). For these standards, concrete countermeasures and combinations of them are missing, which leads to inefficient or even misleading risk mitigation strategies (Fenz et al., 2013).

(2) Standards consists of a huge amount of information. For example, the ISO 27000-series consists of 450 items with 9 focus areas. This complexity and the fact, that there are rarely fully implemented standards in small- and medium-sized businesses in place, leads to a fall back to ad-hoc implementations. An easy to understand toolkit is missing (Mijnhardt/Baars/Spruit, 2016).

(3) The defined controls and countermeasures of the frameworks are often implemented without sufficient consideration of the daily work or their need (Hedström et al., 2011). This is because the organization usually do not consider the relationships between the security concepts (Fenz et al., 2013) and do not check whether a control is really necessary or less critical (Bayuk/Mostashari, 2013; Tu/Yuan, 2014).

(4) Rigorous empirical studies which consider different factors which may affect the decisions and validate the standards and best practices are missing in literature (Siponen/Willison, 2009; Diesch/Pfaff/Krcmar, 2018).

(5) There are regional differences in the use and contexts of frameworks. For example, the NIST SP800-series is “developed to address and support the security and privacy needs of U.S. Federal Government information and information systems” (NIST, 2018b) while the current standard in Australia is the IS0/IEC 27000-series (Smith et al., 2010). Therefore the NIST SP800 framework “is individually useful

but (outside of the U.S.) do not provide a cohesive and explicit framework to manage information security" (Smith et al., 2010).

5.2.2 Information Security Success

Besides standards and best practices which were described before, there are theories and concepts in the literature which help decision-makers in information security. Managers need to know the current information security status of their organizational assets to make decisions. If there are not well protected, they need possible sets of controls with the consideration of the related costs to improve the information security situation (von Solms et al., 1994; Johnson/Goetz, 2007; Tu/Yuan, 2014; Horne/Maynard/Ahmad, 2017; Diesch/Pfaff/Krcmar, 2018).

The literature deals with MSFs to describe the state of information security which is needed in practice. The term was used first in 1987 to describe factors which take into account as "catalysts to generate new and more effective systems security activities" in the security context (Wood, 1987). After that the theory of information systems success of DeLone/McLean (1992) deals with different dependent and independent variables, which are indicating a successful information systems strategy and that they can be categorized into dimensions. Recent studies used other terms in the context of information security:

1. "Information systems security management success factors" are factors to show the state of elements, which has to anticipate preventing information security failure in the e-commerce context (Norman/Yasin, 2013).
2. "Critical success factors" describe factors, which influence the successful implementation of an information security management system (Tu/Yuan, 2014).
3. "Critical success factors are described as key areas in the firm that, if they are satisfactory, will assure successful performance for the organization" (Tu et al., 2018).

In this research, Management Success Factors (MSFs) are defined as factors to show the state of elements, which has to take into account in order to make appropriate management decisions in the information security context of an organization. If the security decisions are appropriate, it assures a successful security performance for the organization.

Current literature mostly looks on factors which influence security separately. To highlight just a view studies, they separately deal with for example organizational factors (Kankanhalli et al., 2003; Ernest Chang/Ho, 2006; Kraemer/Carayon/Clem, 2009; Hall/Sarkani/Mazzuchi, 2011; Narain Singh/Gupta/Ojha, 2014; Mijnhardt/Baars/Spruit, 2016), policy compliance issues (Höne/Eloff, 2002; Boss et al., 2009; Goel/Chengalur-Smith, 2010; Ifinedo, 2012; Lowry/Moody, 2015; Johnston et al., 2016) or human factors (Gonzalez/Sawicka, 2002; Ashenden, 2008; Kraemer/Carayon/Clem, 2009; AlHogail, 2015; Alavi/Islam/Mouratidis, 2016). The reason for the separation is, that security is managed in a separate manner in different departments which includes information security, risk management, business continuity, operational security (Tashi/Ghernaouti-Hélie, 2008). This shows that various studies are available which do discuss different factors in great detail but do not include a integral view on them. There are just a view attempts to consolidate the body of knowledge in comprehensive MSFs. The information systems success theory explains six factors which are contributing to the systems success (DeLone/McLean, 1992). This view does not include specific security considerations including the costs and available countermeasures that a manager must consider. The authors self-criticized the proposed theory because of the missing evaluation. The only other success factor model was a model of factors, influencing the successful implementation of an information security management system (Norman/Yasin, 2013) and not the security decisions of managers itself.

5.2.3 Shortcomings in Literature and Practice

As the Sections 5.2.1 and 5.2.2 suggest, there are a view shortcomings in literature for supporting decisions on the security management level. A recent survey of McKinsey & Company with 1125 managers involved in 2017 identified three main problems, managers face in order to deal with information security issues (Boehm et al., 2018). These are *the lack of structure* within reports with dozens of indicators with inconsistent and too-high levels of details. The *lack of clarity* because of reports, which are too technical which a manager typically not understand. A *lack of consistent real-time data.*

The *lack of clarity* within reports is not just present in practice. Managers do not know all technical details and do not need them because of their teams and experts (May, 1997; Fenz et al., 2013). But they have to establish a security establishment and have to improve the security status by using a security dashboard (Dogaheh, 2010). The reports and dashboards have to be on the need for information security managers (Wilkin/Chenhall, 2010) but there are no standards for the content of such dashboards (Bayuk/Mostashari, 2013). The *lack of structure* is related to the first problem and causes in the high diversity and complexity of the information security problem which causes uncertainty and confusion among top managers (von Solms et al., 1994; Willison/Backhouse, 2006; Savola, 2007; Savola, 2009). This causes in the fact, that managers do not make decisions based on data but on their experience, judgment and their best knowledge (Chai/Kim/Rao, 2011). Therefore, current research asks for a comprehensive approach to information security management (Savola, 2007; Abu-Musa, 2010; Savola, 2009; Savola, 2013; Tu/Yuan, 2014; Nazareth/Choi, 2015; Soomro/Shah/Ahmed, 2016) which captures the definition of "factors that have a significant impact on the information security" (Ransbotham/Mitra, 2009; Leon/Saxena, 2010; Bayuk, 2013; Soomro/Shah/Ahmed, 2016) and the established relationships between these fundamental objectives (Dhillon/Torkzadeh, 2006; Hu et al., 2012; Soomro/Shah/Ahmed, 2016). This research addresses the described needs with the development of the first theory of interrelated MSFs, which give a basis for decision-makers to understand the complexity of information security on an abstract level and also could be the basis of multiple future needs also described in literature like the goal based security metrics development (Johnson/Goetz, 2007; Savola, 2007; Boss et al., 2009; Hayden, 2010; Jafari et al., 2010; Bayuk, 2013; Zalewski et al., 2014; Pendleton et al., 2017; Diesch/Pfaff/Krcmar, 2018).

5.3 Methodology

To develop a comprehensive model of information security factors for decision makers the methodology of this work consists of two steps. Figure 5.1 illustrates the steps. The first step is to find relevant literature with the help of a literature search process described in section 5.3.1. The second step is to analyze the relevant literature for factors which have an influence on information security decisions. The results are categorized and high-level impact factors which are derived from literature. This step is illustrated in section 5.3.2. The third step contains a semi-structured expert interview in order to evaluate the relevance of the impact factors in practice and explore interdependencies between them. The results are evaluated and relevant MSFs in practice as well as interdependencies which results in the comprehensive model of MSFs for decision-makers. In section 5.3.3 the description of the expert interview methodology is shown.

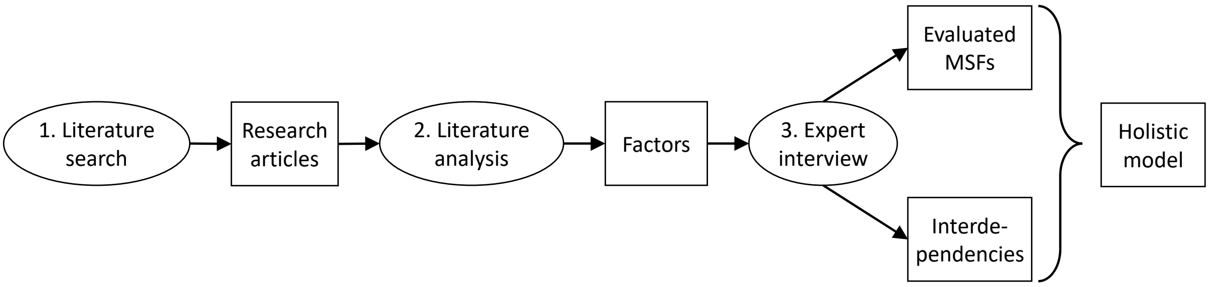

Figure 5.1: *Methodology of theory development*

5.3.1 Literature Search

The search process is performed based on the method of Webster/Watson (2002). The literature search consists of the search scope followed by a keyword-search which ends in a forward and backward search. To provide high-quality articles, the scope is set to highly ranked journals within the information security domain and the information systems management domain because of the relation to the management view. Journals of the management domain were selected from the Senior Scholars' Basket of Journals (AIS Members, 2011). The journals of the security domain were selected from the Scimago Journal & Country Rank (SJR) (SJR, 2018) with the condition that they need to be part of the following categories: security, safety, risk or reliability. To not limit the search only to Journals, the scope was extended to several databases. These are ScienceDirect, OpacPlus and Google Scholar. OpacPlus is a wrapper of multiple databases including Scopus, Elsevier, Wiley, and ACM Digital Library. The results of Google Scholar were limited by 100 hits because the most relevant articles can be found within the first sites (Silic/Back, 2014). After the scope definition, the following search string was used to find articles:

```
(it OR information OR cyber) AND (resilience OR security) AND
(factors OR kpi OR measures OR metrics OR
measurement OR indicator OR management)
```

Listing 5.1: *Global literature search string*

Because the management literature is not information security specific, the search string of these journals was adjusted to the first two parts:

```
(it OR information OR cyber)AND (resilience OR security)
```

Listing 5.2: *Adjusted literature search string*

Another adjustment was done by searching just for the title and abstract within information security specific sources because of the underlying diverse topic. The selection of relevant articles out of the first keyword search was done based on the title and abstract. Including criteria was, that there are factors described or mentioned which are influencing information security decisions. The forward and backward search was applied to all selected articles while the forward search was based on the cited byfunction of Google Scholar. The literature identification methodology results in 136 articles. The complete search matrix with the applied source, the keyword-search hits and the selected relevant article numbers is shown in Appendix A.

5.3.2 Literature Analysis

The analysis was done based on the "open-axial-selective" approach developed by Corbin/ Strauss (1990) which is a grounded theory approach based on Glaser/Strauss (1967). This approach was recommended as a rigorous method for analyzing literature (Wolfswinkel/ Furtmueller/Wilderom, 2013). This approach has the advantage, that the whole context of an article can be analyzed in order to extract factors. Webster/Watson (2002) also support a literature analysis but with the categorization of a whole article in order to identify gaps in the literature, pointing out the state of the art and explaining past research. To extract specific knowledge and categorize this, the coding on a textual level of articles is more appropriate in this case. The coding follows the following steps:

(1) Assignment of text segments to a "first-order code". For example, the text segment "those organizations that have had a systems security function for some time should use these assessment methods to validate the results of other methods and to cross-check that they have not overlooked some important vulnerability" (Wood, 1987) was assigned the cluster "vulnerability assessment" as a factor which influences information security.

(2) Combines synonymous and their meanings to a "second-order code".

(3) Categorize the "second order codes" to clusters based on overlapping meanings (infrastructure overview and asset knowledge), overlapping functions (management support and management standards) or theoretical constructs (confidentiality, integrity, and availability).

5.3.3 Expert Interview

Previous research has been criticized in order of missing support of reliability and validity by empirical studies (Siponen/Willison, 2009; Tu/Yuan, 2014). The first goal of the expert interview was to evaluate the factors of the literature and thus generate MSFs which are relevant in practice. The second and main goal is the exploration of interdependencies between MSFs to develop the comprehensive model of MSFs.

There are various ways to design an expert interview. This study is designed as a semi-structured interview (Bortz/Döring, 1995) to combine the advantages of structured and open interviews. The interviewer is able to give room for explanations but also ensures, that all answers are given. With these considerations, the expert interview itself consists of three steps which are the operationalization of the described goals (Section 5.3.3.1), the selection of experts (Section 5.3.3.2) and the analysis of the expert interviews (Section 5.3.3.3).

5.3.3.1 Operationalization

The interview guide gives the interviewer an orientation and an analysis is more comparable than without any structure. To develop the survey instrument, the rules of good expert interviews were considered (Bortz/Döring, 1995). The beginning of the interview was done with an open question on the most important factor, the interviewee considers for the information security in the organization (*Q0*). The following areas were discussed with the experts to support the given goals and control as well as confirm the validity of the factors:

- Evaluation of factors:
  A discussion about the meaning of each factor from a practical perspective was done in order to evaluate the content of the factors (*Q1.1*). The practical relevance was tested by asking about the importance of each factor for the information security of the organization (*Q1.2*).
- Exploration of interdependencies:
  To explore the interdependencies between the factors and get insights into them, a discussion about the practical usage and how the experts deal with each factor was done (*Q2.1*). To crosscheck the given statements, experts were asked for each factor, if the factor has a direct impact on the information security of the organization (*Q2.2*).
- Control questions:
  Questions about the absence of not mentioned important factors (*Q3.1*) and if the experts consider a factor which was discussed to be unimportant (*Q3.2*) are used to control the completeness of the given factors and further confirm the explored results.

5.3.3.2 Expert Selection

An expert is a person with specific practical or experimental knowledge about a particular problem area or subject area and is able to structure this knowledge in a meaningful and action-guiding way for others (Bogner/Littig/Menz, 2014). The selection of interviewees was derived by this definition. Therefore, an expert should have several years of experience in the field of information security which points to specific practical knowledge in the field of information security. The expert should have a leading position within the organization which testifies the ability to the meaningful and action-guiding structuring of the information for others. Also, a leading position supports the underlying comprehensive view which is required for the goal of this research. The selection results in 19 participants. They were mainly Chief Information Security Officers (CISOs) (12) and Information Security Officers (ISOs) (4). The others were one Chief Executive Officer (CEO), one Chief Information Officer (CIO), and a technical delivery manager. All experts had 5 years of experience at minimum, 16 years at average and 30 years at maximum. This shows, that the selected interviewees meet the requirements and are suitable for this approach. The participants worked in the following industries at this point in time: finance, automotive, diversified, aircraft, metal and electrical, services, hardware and software, and others. All but one organization had more than 2000 employees. This was the result of the requirements for experts which mean, that the organization has to had at minimum an information security team, which is typically not available in small businesses.

5.3.3.3 Interview Analysis

The interviews were analyzed according to Mayring (2015). The basis for each question was a full transcript of the interview. The process contains of the following steps:

1. Paraphrasing
   - Deletion of components that do not contribute or have little content.
   - Standardize language level.
   - Generate grammatical short forms.
2. Generalization
   - Generalize paraphrases on an abstract level.
   - Generalize predicates in an equal form.
   - Generate assumptions in case of doubt.
3. Reduction (can be done multiple times)
   - Delete phrases which have the same meaning.
   - Combine phrases of similar meaning.
   - Select phrases that are very content-bearing.
   - Generate assumptions in case of doubt.

To analyze quantitative aspects or interdependencies, Mayring (2015) also suggests two methods which are called “valence or intensity analysis” (V) and “contingency or interrelation analysis” (I) and used to analyze the interviews. Both methods contain mainly the same steps:

1. Formulate a question.

2. Determine the material sample.
3. Define the variables (V) / text modules for interrelation (I)
4. Define the scale (V) / rules for interrelation (I)
5. Coding
6. Analysis
7. Presentation and interpretation

5.4 Management Success Factors

The prerequisite for a comprehensive model of MSFs is evaluated MSFs, which have an influence on information security decisions. In Section 5.4.1, the results of the literature analysis are shown. These are factors which have an influence on information security decisions from the literature perspective. After that, the factors have to be evaluated and proved for their relevance in practice which results in evaluated MSFs. These results are shown in Section 5.4.2.

5.4.1 Factors Derived from the Literature

The analysis of 136 relevant articles from the search methodology resulted in 188 first-order codes. A code is a tuple of “factor in literature”-“author”. So for each author, the different impact factors were coded. These codes appear in the following situations:

(1) They appear **directly** within the literature. An example is the following sentence of Atoum/Otoom/Abu Ali (2014) “enrich the framework in other related dimensions such as *human resource*, *organization structures*, *global governance*, *regulation regimes*, *awareness programs* and thus provide a more detailed framework”. This result directly in the corresponding list of first order codes. Most of these direct codes appear in enumerations within the introduction or future work sections of the analyzed literature and are not further explained.

(2) The first order codes are part of a **theory**. The first order codes are part of a hypothesis construct with a underlying theory and are tested with quantitative or qualitative studies. A example work is Kankanhalli et al. (2003) which describes the impact of the organizational size, the top management support and the industry type on the information systems security effectiveness. This example results in the corresponding first-order codes.

(3) **Indirectly** within the articles or because of their focus. These appearances are derived from the overall classification of the articles or some descriptions within the text which are not directly mention the first order code but the meaning was chosen to name it. The article with the title “design and validation of information security culture framework” (AlHogail, 2015) is named “security culture” as a first-order code. A other example for indirect mentions is “those organizations that

have had a systems security function for some time should use these assessment methods to validate the results of other methods and to cross-check that they have not overlooked some important vulnerability" (Wood, 1987) which is "vulnerability assessment" as a first-order code.

The aggregation of the 188 first-order codes results in 44 second-order codes. The following aggregation criteria were identified:

(1) Articles describe often, that the codes have the **same meaning**. An example is given by Jafari et al. (2010) which described "Safeguards: Protective measures prescribed to meet the security requirements [...], synonymous with countermeasures". This in conjunction with "improving the overall information security state by selecting the best security countermeasures (controls) to protect their information assets" (Yulianto/Lim/Soewito, 2016) are safeguards, countermeasures, and controls a second-order code.

(2) Certain first-order codes are **part of** or included in other first-order codes which results in a second-order code. Examples in literature are "Value delivery (i.e. cost optimization and proving the value of information security)" (Yaokumah, 2014), "aside from the personnel measures which focus on human behavior" (Sowa/Gabriel, 2009) or "threats, which form part of such risk" (Willison/Backhouse, 2006). This indicates, that threats are part of risks.

(3) First-order codes are aggregated in order of their **underlying object**. An example is "organizational size", "industry type" and "organizational structure" which are all features of an organization and thus are aggregated to the second-order code "organizational factors".

The aggregation of the second-order codes to clusters and thus the overall factors, influencing security decisions, is based on common theories in literature. An example is the theory of the protection goals of information security which is supported by various authors: "with a goal to compromise Confidentiality, Integrity and Availability (CIA)" or "it also coincides with the Confidentiality-Integrity-Availability (CIA) framework" (Goldstein/Chernobai/Benaroch, 2011) or "one view, which gained especially wide popularity, is called C-I-A triad" (Zalewski et al., 2014). This theory results in the consolidation of protection goals in the factor "CIA".

The result of the literature analysis is 12 factors influencing security decisions, namely: "Vulnerability", "Compliance & Policy", "Risk", "Physical security", "Continuity", "Infrastructure", "CIA", "Security management", "Awareness", "Resources", "Access control" and "Organizational factors". The detailed codes and the aggregation steps are available in Appendix B.

The literature analysis confirms the assertions made in Section 5.2.3 which say that various individual factors are mentioned, enumerated or examined. However, up to now, there has been no comprehensive view on them, a discussion of the practical relevance is missing and the interdependencies of the factors among each other are not described. The result of this chapter gives an abstract view of current factors in literature, influencing information security decisions.

5.4.2 Evaluation of Factors

The explored factors of the last Section 5.4.1 are the basis for the following evaluation and therefore to transform these factors to MSFs for information security decision-makers. In Section 5.4.2.1 the practical view of experts on the factors is compared to the literature view which is derived out of the literature analysis in Section 5.4.1. In addition, challenges of practitioners are supported for each factor. The result of the relevance validation is present in Section 5.4.2.2. Section 5.4.2.3 contains the result of the control questions and thus confirm the validity and relevance of the explored factors.

5.4.2.1 Content Validation of MSFs

The relevance of the factors in practice and their validity makes them to MSFs. The general context analysis (Section 5.3.3) was used to determine the practical usage and meaning of the different factors out of the literature. To analyze them, the scope was set to the whole interview transcripts while the main answers are given by the guiding question *Q1.1* of the interview guide. Because of the methodology design of a semi-structured interview, the challenges and problems of each factor in practice is a side-result and also reported here. The following itemization shows each MSF with a description of the literature view, a consolidated practical view and the challenges practitioners face regarding each MSF. The literature view is a consolidation of definitions and opinions out of the literature analysis 5.3.3.3. The practical view and the descriptions of the challenges are a consolidation of the main opinion of all 19 experts.

- **Vulnerability**

    1. **Literature:** The definition of a vulnerability in literature is generally a “weakness of an asset or control that can be exploited by one or more threats” (ISO/IEC, 2018). This definition is very generic and can be technical as well as non-technical. NIST gives a more detailed definition as a “weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source” (NIST, 2018a). Common usage of the term in the analyzed literature is, that vulnerabilities are technical in nature. More specifically, “a vulnerability is a software defect or weakness in the security system which might be exploited by a malicious user causing loss or harm” (Joh/Malaiya, 2011).
    2. **Practice:** Vulnerabilities from the management perspective are always technical in nature. Specifically, known vulnerabilities within systems and software are meant by them. The common understanding of the experts was that vulnerability is a topic of patch management and a problem of not patched systems. All organizations do have patch management in place and try to minimize the vulnerabilities in the infrastructure. The assessment of them is done with vulnerability-scanners, penetration-tests, automatic scans, audits

and the definition of toxic software which is detected on systems. Patching and the elimination of vulnerabilities are done based on the given assessment methods.

3. **Challenges:** A problem is, that the vulnerabilities have to be known first. Not just the knowledge of the vulnerabilities is a problem but also the knowledge of the assets and the whole infrastructure of an organization is a challenge in practice. Just if an organization knows the whole assets and infrastructure, it is possible to determine, if there are known vulnerabilities or not.

- **Infrastructure**

  1. **Literature:** Infrastructure does have different aspects. Components are technical systems which itself try to protect the underlying assets or are there to identify attacks. Examples are firewalls, intrusion detection systems, information visibility, compromise detection, defense modeling, and other solutions. A second important concern is the prevention of attacks without any known vulnerabilities. This includes architectural decisions to segment the network, limit open access points or external connections, harden the systems, encrypt the communication or clean configuration issues. Since these are no specific vulnerabilities but considered as weaknesses, this topic is a stand-alone factor.
  2. **Practice:** Some of the experts see this factor as a vulnerability-topic but most of them associate more than that with the infrastructure factor. It is about knowing all systems and software as well as the connections between them and if they are secured or not. It is also about the "hardening" of all available systems, make threat models and secure the infrastructure in each network layer. To accomplish that, the experts use hardening-guidelines, secure deployment, installation routines, design reviews and configuration management databases.
  3. **Challenges:** Problems are the complexity of the activity, that it is difficult to check the wright implementation of the hardening guidelines and the above-mentioned problem of the difficulty to know all available systems and their connections.

- **Compliance & Policy**

  1. **Literature:** Security policies are an "aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information" (NIST, 2013b). All activities concerning compliance and policies like policy deployment, policy effectiveness, legal compliance, and regulatory requirements are subsumed in this factor. The literature describes also multiple characteristics for good and bad policies and controls which have an influence on the information security of organizations.
  2. **Practice:** This factor means the implementation of requirements which are given from external and internal. These include laws, policies from the management and requirements from standards to get certificates. Practitioners use frameworks to implement them and audits as well as self-assessments to check them. This frameworks and policies help organizations which have not the common knowledge to consider all aspects of security.

3. **Challenges:** 100% compliance does not mean 100% secure. This factor alone does not help in case of security but without, it is not possible to make audits or push measures through.

- **Security management**

  1. **Literature:** This factor subsumes all process activities within the information security management system and operational tasks like change management, incident management, process effectiveness measurement and the implementation of security standards. All aspects of the Plan-Do-Check-Act approach of the ISO/IEC 27000 (ISO/IEC, 2018) are part of the security management factor. The other part are strategic topics like goal definition, top management support, governance, and strategic alignment as well as the documentation of these activities. Also, an important aspect in literature is the communication with employees and the top management. The ISO/IEC 27000 defines security management as a “systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization’s information security to achieve business objectives” (ISO/IEC, 2018). This definition shows that the monitoring part is also established within this factor. There are different methods and processes described to continuously improve the information security of an organization. This covers the implementation of metrics and the topic of compromise detection.
  2. **Practice:** There are two management approaches in place. The risk-based and the control-based approach. There are various processes in place to support the two different approaches. Therefore the experts control their management processes with audits and using the Plan-Do-Check-Act framework from the ISO/IEC 27000 (ISO/IEC, 2018). The next important aspect for the interviewees was the business (top) management support and their understanding of the risks the organization is facing.
  3. **Challenges:** A problem is the missing knowledge of concepts behind the security processes and also the lack of knowledge of available actions for improvements. The security management does not have an impact on the security of an organization without this knowledge.

- **Awareness**

  1. **Literature:** The definition of awareness in literature is to be aware of security concerns (NIST, 2013b). Awareness in academic literature is discussed in different subjects. Including in this factor are behavioral topics like employee behavior, user activities, user interaction but also user reaction, user errors, and faults. All parts depending on knowledge like skills, education, training, and competence are also including in the awareness factor. Awareness in literature is not just about peoples behavior but also the personal needs of them, privacy issues, trust concerns as well as cultural thoughts and the social environment.
  2. **Practice:** All topics that concerning people and can not be treated with technology are subsumed by awareness. Typical understanding is the employee as a vulnerability with human errors, human behavior or not enough knowledge. A typical countermeasure is web-based and conventional training. Practitioners test their employees with own phishing-campaigns or check click-rates on

their proxy-servers. Cultural and privacy concerns are not often taken into consideration.

3. **Challenges:** Challenge in practice is, that awareness activities are very resource heavy and the effects are not that huge. Countermeasures often do not lead to measurable effects, they lead to annoyed employees and therefore, employees more often fail the same tests.

- **Risk**

  1. **Literature:** The risk factor is discussed as an overall risk management concern with possible threats, the likelihood of their occurrence and the possible impact on the organization. Literature mostly discusses the risk management process and the possible handling of present risks like prevention, tolerance, exposure, prediction, and perception. A comprehensive definition is given by the NIST SP800-37: “A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence” (NIST, 2018a).
  2. **Practice:** Experts use the same definition and understanding of risk as in literature. A risk is a severity and likelihood combined with an issue. Information security is the applied risk management because it is used to prioritize and define countermeasures. Therefore, all of the experts have risk management based on certain standards like ISO/IEC 27000 or NIST in place.
  3. **Challenges:** Not all risks can be mitigated, because of missing resources or other restrictions. Some managers also have problems to define risks which are understandable for technical employees or even for the top management. Also, the availability of the underlying data is a challenge in practice. An example of this is the consolidated view on possible threats. There are various technical solutions like threat intelligence platforms available on the market which helps to consolidate these data. The problem comes with the combination of the different factors to define the risk. A possible threat alone is not important for the information security management. The challenge is to analyze the underlying assets and their vulnerabilities and check if the threat can exploit one of these. After this combination, the risk can be defined and is useful for an information security manager.

- **Access control**

  1. **Literature:** Access control is not mentioned as a part of countermeasures. This topic is such important that it often emerges as an independent and important factor for security. Access control contains account management, software access control as well as access rights. It means “to ensure that access to assets is authorized and restricted based on business and security requirements” (ISO/IEC, 2018).
  2. **Practice:** Access control is the management and regulation of access to systems, applications, data, and infrastructure. It is not just about the access but also the key management, role administration, classification of data and the management of the identities within organizations. Therefore the experts

have procedures per applications, try to implement the common principles like the need-to-know- or the least-privilege-principle. They check the available accesses, have identity and access management in place and use tools to monitor them.

3. **Challenges:** Challenges occur in case of on-, off-boarding and department changes as well as the more and more open culture of organizations with “bring your own device” and “cloud infrastructure”. Not just the open culture but also technologies and trends like the “internet of things” and “mobile devices” are increasingly a problem for this factor because each of these devices also has an identity. This increases the complexity of managing access control and has to be considered by choosing such technologies.

- **CIA**

  1. **Literature:** This factor is based on the overall theoretical construct of the protection goals of information security. Therefore the codings confidentiality, integrity, availability, as well as underlying goals like the non-repudiation, are subsumed in this factor. Articles about security metrics and security success are mostly based on this factor and plays a huge role in the security discussion.
  2. **Practice:** In practice, this factor is a theoretical construct with the same definition as in literature. It is used to communicate with the business management, to classify the need for protection or is not used in practice at all.
  3. **Challenges:** The problem in practice is that these classes can not be uniquely assigned to countermeasures. Many experts consider this factor as an academic construct, which is outdated and not really practicable.

- **Organizational factors**

  1. **Literature:** The organizational factor itself means the properties of an organization which has an influence on the security of this organization. There are multiple authors which mentioned the influence of several factors like the organizational size, the industry type or the internal and external structure of the organization.
  2. **Practice:** These factor has the same meaning in practice like in literature. Most of the experts are not dealing with it because there are no possibilities to change the characteristic of the organization from their perspective. But it is considered in other factors like risks or in consideration of the implementation countermeasures. Practitioners say, that it might influence the possibilities of an organization.
  3. **Challenges:** A challenge is, that some attack surfaces are not influenced by any type of character an organization could have. A good example of this is ransomware which does not even look at the victim they attack.

- **Physical security**

  1. **Literature:** This factor have influence in reducing the opportunity to access assets physically in form of physical entry controls, the protection of the environment, building security with fences or other countermeasures, travel

security and all activities around this. The literature does not mention this factor very often but consider it as really important for organizations and their management.

2. **Practice:** Physical security is the physical protection of buildings, offices, servers, and hardware. It also contains the protection of the environment, persons, traveling and environmental disasters. Interviewees do work together with other departments dealing with this factor. It is mainly not the part of the security department of an organization.
3. **Challenges:** The topic gets less important in times of the changing environment like mobile offices, roaming-users, home offices and cloud computing. This change brings with it other challenges.

- **Continuity**
  1. **Literature:** Continuity is split in business continuity and IT continuity. In case of cyber security, the term "refers to the ability to continuously deliver the intended outcome despite adverse cyber events" (Björck et al., 2015). The business continuity is on a more abstract level than cyber or it continuitiy and is defined as a "predetermined set of instructions or procedures that describe how an organization's mission-essential functions will be sustained [...] before returning to normal operations" (NIST, 2013b). Resilience is not often represented in the literature and has already been identified as a research gap (Diesch/Pfaff/Krcmar, 2018).
  2. **Practice:** This factor is understood as the goal of the business as well as a partial goal of information security. Important is a continuous IT and a disaster and recovery plan which should be tested from time to time. There are opposite opinions in relation to Business Continuity Management (BCM). Some experts say, that requirements come from the BCM to the information security management and others say, that they are being submitted to the BCM.
  3. **Challenges:** A challenge is finding a common understanding and effective communication between BCM and IT continuity.

- **Resources**
  1. **Literature:** Resources are not just money but also the availability of good skilled and well-educated employees. More general resources are "information and related resources, such as personnel, equipment, funds, and information technology" (NIST, 2013b). The literature describes this factor as a limitation and mostly in a negative way. The perspective is given that, if you do not have enough resources, the organization is not able to implement security which as a negative influence. A second part is the cost-effectiveness of countermeasures and the Return on Security Investment (ROSI).
  2. **Practice:** In practice, this factor is mostly addicted to budget, which has to be given by business management. A small part is also the number of employees with good knowledge and a appropriate education. Therefore, experts have applied budget-processes and recruitment campaigns. Cost-effectiveness and ROSI is not mentioned by the practitioners.

3. **Challenges:** Problems are often in place of buying expensive tools and equipment in the security field and the argumentation of their adding value. It is often a tension between business management and security management.

Partial aspects of individual factors are not covered by the literature or are not considered in practice. However, the contents and the understanding of the factors from the literature analysis agree with those of the experts. The challenges are not supported by all of the experts, because this was no explicit question. Thus, they were just included, if there are more than 2 mentions of the same challenge. The challenges further indicate, that a comprehensive model of them could help, improving the understanding of information security within organizations and also to help, improving specific factors.

5.4.2.2 Relevance Validation of MSFs

The "valence or intensity analysis" (Section 5.3.3) was used to not just validate the factors concerning their content but also to determine their relevance in practice to the information security of an organization. Therefore, the scope of the analysis was also set to the whole interview transcripts but the main question supporting this validation is *Q1.2*. A 4-point Likert-scale which points out the importance of the factor for the information security of the organization is used. The coding of the scale is from not important (not imp) to important (imp). Table 5.2 shows an assorted view of the result. The assortion is based on the sum of the codings for "not important" and "rather not important" in conjunction with the sum of the coding "rather important" and "important", descending by the importance of the MSFs.

MSF	**not imp**	**rather not imp**	**rather imp**	**imp**
Vulnerability	0	0	7	12
Resources	0	0	7	12
Awareness	1	0	6	12
Access Control	0	1	8	10
Physical Security	1	0	11	7
Infrastructure	0	1	12	6
Risk	0	1	12	6
Continuity	1	1	13	4
Security Management	3	1	8	7
Organizational	3	4	11	1
CIA Triad	7	1	8	3
Compliance & Policy	6	3	7	3

Table 5.2: *Importance of MSFs for the IS of organizations (number of experts)*

This result support, that all factors are relevant in practice. The last three factors are "Organizational factors", "CIA" and "Compliance & Policy". For all of them, the experts do have an explanation, why they are less important than the other factors. "Compliance & Policy" are not important for the information security of the organization itself but are necessary to comply with the law, to enforce countermeasures and to align the top management of the organization. The "CIA" factor is a goal factor and is useful to communicate and explain different risks or attacks and their impacts. “Organizational factors” are less important because there are cases, in which these factors are important but there are also attack scenarios in which this factor is not important. The management has to consider all the factors in order to make good decisions. The proposed factors are valid in their context as well as relevant in practice for decision-makers and thus are now called Management Success Factors (MSFs).

5.4.2.3 Control Questions

The main control questions *Q3.1* and *Q3.2* are used to ask for factors, which are important to make decisions and are not present in the interview guide as well as a consideration of the most unimportant factor. The most experts (12) do not have a factor, which is really unimportant. The only mentions of factors were the “Compliance & Policy” as well as “CIA” which agree with the ranking on the previous result. The question of missing factors results in a similar situation like before. 10 experts do not mention missing factors. The other factors which are missing are “management support”, “external interfaces”, “threat landscape” and “strategy” which are part of the coding and thus included in the aggregation of the literature analysis.

5.5 A Comprehensive Model of MSFs

The purpose of this research was the development of a comprehensive model of MSFs for information security decision makers. This result section combines the previous results with evaluated and relevant MSFs and adds interdependencies between them. The interdependencies were explored with the help of the “contingency or interrelation analysis” method (Section 5.3.3). The scope is the whole interview which was analyzed. The following text modules are examples to identify interrelations:

- ... have a direct impact on ...
- ... is a basis to ...
- ... is essential for ...
- ... is the goal from ...
- ... is considered in ...

Figure 5.2 shows all MSFs with their interrelations based on the expert interview. Solid ovals are representatives for the MSFs. Dotted ovals are representatives of concepts necessary to explain certain interdependencies. In this case, “Information security” is the representative for the information security status of an organization. The statement behind this is, that certain factors do have a direct impact on the information security status of the organization. The dotted oval “Countermeasures” is a part of the factor “Security management” but have important interdependencies which are explained by the experts. Thus, the security management itself does not have a huge impact on other factors, but they define and implement countermeasures which do have an influence on the MSFs given in the figure. Rectangles within the picture clusters multiple MSFs with the same interdependency to other MSFs. The dotted line within the rectangles indicates, that all MSFs which are left of this line, are not the primary part of the information security department of an organization. They are from other departments like the cooperate-security in the case of "Physical security" and the business continuity in case of "Continuity". However, the collaboration between the departments is very close and the MSFs must certainly be considered in information security as well.

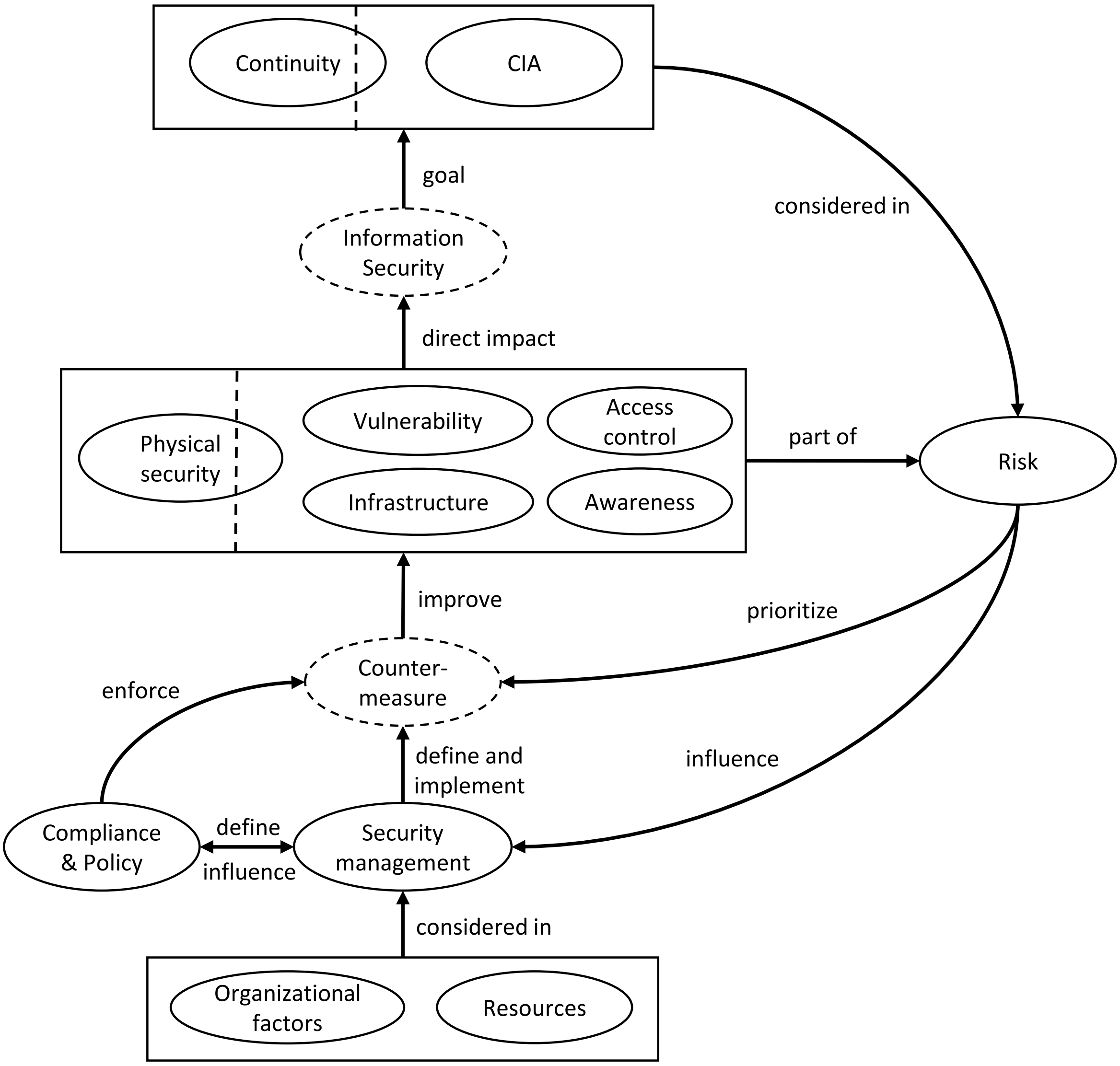

Figure 5.2: *A comprehensive model of MSFs for information security decision-makers*

Key security indicators. The term key security indicator is not present in literature but is mentioned by practitioners. Key security indicators are MSFs, which have a direct impact on the security status of the organization. Therefore, the rectangle which includes the MSFs "Physical security", "Vulnerability", "Access control", "Awareness" and "Infrastructure" are key security indicators. Because of the direct connection to the information security concept, these factors are considered as indicators of the actual information security status of an organization. Security management has to implement countermeasures to actively improve these factors. These are the most important factors because of their direct impact.

Security goals. The MSFs “Continuity” and “CIA” are the protection goals of information security. This cluster is considered in the “Risk” MSF by data classification as well as a communication instrument which describes the impact of certain risks to top managers or technical employees. Disasters and continuity thoughts are also considered as risks which are the basis for recovery plans. The security goals are considered as the least important part of the MSF model by experts (Section 5.4.2.2) because they do not actively improve the security status and just help by prioritizing risks and communicate them to the business management.

Risk. The MSF “Risk” have the most interrelations and is the basic input for “security management”. It uses security goals like described before. A prerequisite and a part of risks are key security indicators. They show the current information security status of which weaknesses were deriving. This, in combination with possible threats, the impact on the organization, and the likelihood of occurrence is a risk. Risks are influencing the “Security management” and is a basis to prioritize and define “Countermeasures”. The management mostly uses standards and best practices like the ISO/IEC 27000 (ISO/IEC, 2018), NIST SP800-30 (NIST, 2015), NIST SP800-37 (NIST, 2018a) or others to deal with risks and derive countermeasures in a structured way.

Security management. The cluster with “Organizational factors” as well as “Resources” are MSFs which cannot be directly influenced by the experts. They are either given in case of “Organizational factors” or are set by the business management in case of “Resources”. They are considered in the “Security management” in conjunction with the “Risk” MSF which are the basis to develop and implement countermeasures which should improve the key security indicators. “Compliance & Policy” are aids which help to enforce countermeasures with employees and are necessary to comply with laws. “Compliance & Policy” is split into external and internal rules which causes the interdependency in both ways to and from the “Security management” MSF. “Security management” define rules and external rules are influencing the “Security management”. These rules are considered as the least important by the experts (Section 5.4.2.2) because they are not actively improving the security situation but are helpful to enforce countermeasures and help to deal with the topic.

5.6 Discussion and Future Research

The results of this research propose a comprehensive model of MSFs with their interdependencies for information security decision-makers. The MSFs were supposed based on the literature and are evaluated by experts from practice. These interviews also support interdependencies between the MSFs. The combination of these results in the development of the comprehensive model of MSFs.

Practitioners, as well as the literature, stated the need for a comprehensive view of the information security of organizations. The proposed model does support an abstract and comprehensive view of the complex topic of information security from the management perspective. The different MSFs are not explained in great detail but the interdependencies between them and the overall decision-making process are present in this research. The model gives a basis to decision-makers, which with information security management and help to decide if certain countermeasures are necessary or even useful. It is not just a basis for security managers but also for the business management as well as technical employees. With the help of this model, they are able to understand the difficulties and retrace certain decisions better. A better understanding also leads to better alignment and awareness.

The results are related to several other studies. Past literature does support a great explanation and study of different factors in detail and stated the importance of them. Studies also deal with models of different factors like awareness and their components. This research supports a comprehensive overview of high-level factors (MSFs) and a validation of them as well as a discussion of the relevance of these factors which has been criticized as missing in past articles. The research adds value to the research community by exploring interdependencies between the evaluated MSFs and propose a comprehensive model from the perspective of information security decision-makers. Best practices and standards are very generic and mostly describe processes. But, a complete implementation does not necessarily lead to better security and the standards have been criticized, also by experts in the interview, that they are just frameworks to be compliant. The interdependencies of the comprehensive model in this research help to decide which countermeasures are appropriate and which are not necessary. The standards and best practices give action proposals for improvements of the MSFs and thus complete this research with the next step after the decision was made.

Current standards and best practices, for example, the ISO/IEC 27000-series, the NIST SP800-series or the ISF are important to structure the processes of improving the information security of an organization. These documents either describe processes based on a risk management approach to implement countermeasures or define controls which have to be implemented to comply with the standard. The most experts in the interviews said that they combine two or more of them and uses the concepts they need or are appropriate for them to improve the information security status of the organization. The proposed model in this research contributes to these standards by improving the overall understanding and the interdependencies between the concepts described in the standards. Also, the model is a possibility to report the information security status based on the MSFs. Such a reporting is missing in the current standards and best practices as well as in research articles. The missing reporting standard or suggestions for that is a need which all of the interviewed experts have. Experts also struggle to report the information security decisions and status to the business management in an abstract and understandable way. The current solution of the interviewed experts is that they develop their own reporting standard. These reports do not contain aspects which can be compared with other businesses or even business units. The results of this research support these needs and can be used as a basis for such a reporting standard. Experts also looking for dedicated technical solutions like threat intelligence platforms, security incident management systems and information on indicators of compromise to mention just three. These technologies help to consolidate various information and present them to the management. Each technology is useful for a specific area. This research can help to argue the implementation of specific technologies, to illustrate their role in the overall security context and to identify gaps within the security landscape of an organization in which technologies could help.

The result can also be interpreted from the perspective of the information security status of an organization. From this perspective, the model indicates, that the key security indicators are important to improve the information security status of the organization. This interpretation in mind, small- and medium-sized businesses with fewer resources and not that much competence could implement light-weight countermeasures, which focus on the key security indicators. It could be a quick-win for the decisions in those organizations to focus on the key security indicators. This does not mean, that the standards and best practices or even the other factors of the model should be ignored by small- and medium-sized business. To continuously improve and monitor the information security status in a structured way, the processes and concepts of these standards have to be implemented and used. The proposed model can help these businesses and their management with less expertise in the field of security to understand the interdependencies between relevant concepts, understand which factors are influential and also which factors a manager has to consider by making decisions. Even which factors have to keep in mind to make well-informed decisions.

This study uses a mixed method approach with a literature analysis followed by a semi-structured interview to generate the results. Although a rigorous methodology was used, the study has several limitations. Despite the validation and the discussion with experts, a bias in the interpretation of the texts and the creation of the codes cannot be excluded. Surveyed experts are mainly active in large organizations. Some of them were previously employed in smaller businesses, but the inclusion of opinions from managers of smaller organizations could change the outcomes and importance of individual factors.

The results give many opportunities for future research. The proposed model is based on interdependencies, which are explored by a qualitative study. The interdependencies should be further tested with quantitative approaches to ensure their validity. Certain MSFs were clustered into rectangles. There could be interdependencies between the containing MSFs on deeper levels, which are not be explored in this study. Also, a look deeper within the certain proposed MSFs would be a possibility for future research. Open question from past literature could be solved with a more focused approach based on this results. Leon/Saxena (2010) identified a gap of the security metrics approach, which was not goal-focused in the past and suggested the development of a goal-list which could improve further security metrics development. This comprehensive model and their MSFs could be considered as a list of security goals from the management perspective and thus can be the basis of such research. Also, past metric approaches are mainly based on the individual security processes and thus is not appropriate for cross-organizational comparisons (Bayuk, 2013). A metrics approach based on a comprehensive model could be suitable for this. Also, the interview partner requested a dashboard and reporting standard for key security indicators which is not present in standards, best practices or research articles. To reduce the shortcomings, a future study is possible, which includes small- and medium-sized businesses and integrate them in the proposed model.

Information security managers should consider all the explored MSFs by taking decisions. The countermeasures and processes should not only be adopted because of their appearance in standards and best practices, but they should appropriate in the given situation. A common practice is also the fallback to risk acceptance (Bayuk, 2013) which do not improve the security status at all but is very easy to implement. The results of this study facilitate the understanding of the complex topic of information security and enable more people to make appropriate decisions and take the right actions within their current situation.

5.7 Conclusion

This research is suggesting a comprehensive model of management success factors (MSFs) for information security decision-makers. Therefore, a literature analysis with an open-axial-selective approach of 136 articles is used to identify factors which have an influence on the information security decisions of managers. A validation of these factors, as well as the check for their relevance, was supported by conducting an interview series of 19 experts from practice. This results in 12 MSFs. To finally develop the comprehensive model, the interviews are the basis to explore interdependencies between the MSFs.

This research suggests that “Physical security”, “Vulnerability”, “Access control”, “Infrastructure” and “Awareness” are key security indicators which have a direct impact on the information security status of an organization. The “Security management” have to consider “Risks”, “Organizational factors” and available “Resources” in order to generate countermeasures, which have an influence on the key security indicators. “Compliance & Policy” is an aid to enforce countermeasures and be compliant with laws. The well discussed MSF “Risk” is considering the security goals “CIA” and “Continuity” and also is using key security indicators to determine a risk level which is used to prioritize countermeasures.

This research offers a high-level view of the complex topic of information security decision-making from the perspective of security management experts. The comprehensive model of MSFs helps them and other employees as well as the business management to better understand the security needs and certain decisions in this context and thus improve their awareness. Future development of goal-oriented metrics and methods to quantify the status of information security as well as methods to aggregate them based on the key security indicators are not just interesting in research but also asked by practitioners.

6 Linking Information Security Metrics to Management Success Factors

Title	SoK: Linking Information Security Metrics to Management Success Factors
Authors	Diesch, Rainer[1,2] (diesch@fortiss.org) Krcmar, Helmut[2] (helmut.krcmar@tum.de) [1]fortiss GmbH, Guerickestraße 25, 80805 Munich, Germany [2]Technical University of Munich (TUM), Boltzmannstraße 3, 85748 Garching, Germany
Type	Conference and Proceedings
Outlet	ARES 20: International Conference on Availability, Reliability and Security
Publisher	ACM's International Conference Proceedings Series (ICPS)
Ranking	CORE 2018[3]: B
Status	Published
How to Cite	Diesch, R.; Krcmar, H. (2020): SoK: Linking information security metrics to management success factors. 15th International Conference on Availability, Reliability and Security (ARES 2020). Virtual Event, Ireland, pp. 1–10, doi: 10.1145/3407023.3407059
Individual Contribution	Conceptualization, Methodology, Investigation, Data Curation, Writing - Original Draft, Writing - Review & Editing, Visualization

Table 6.1: *Bibliographic details for P3*

[3] http://portal.core.edu.au/conf-ranks/923

SoK: Linking Information Security Metrics to Management Success Factors

Abstract: Information security metrics are used to measure the effectiveness of information security countermeasures. A large number of metrics and their technical nature creates difficulties when generating reports for the information security management level of an organization. Managers struggle with the usefulness and clarity of the metrics because they are not linked to the security management goals. Also, responsible managers with no technical information security background struggle to understand the metrics. Therefore, this study uses a state-of-the-art literature analysis together with the Goal-Question-Metric approach to investigate linking technical security metrics to management success factors. This study enables the management to design appropriate security reports for their organization and to direct the metrics toward making goal-oriented decisions. Furthermore, the study invites future research by revealing areas in which security metrics do not exist and create new solutions and studies to suggest a standardized information security dashboard.

6.1 Introduction

Information security is one of an organization‘s most important issues. If an organization does not deal with information security, the repercussions affect not only finances but also the firm‘s reputation and legal standing (Tu/Yuan, 2014). Therefore, various standards and best practices like the ISO/IEC 27000 series (ISO/IEC, 2018), the NIST 800 series (NIST, 2018b) or other national and international frameworks like COBIT (ISACA, 2012) or ITIL have been put in place. These standards all deal with metrics and measurements for the implementation and further improvement of the information security management within organizations.

An information security assessment is one of the most important activities conducted by information security management and technical information security employees. Audits or security metrics are the methods used to assess an organization‘s information security status. Because information security can not be measured directly (Zalewski et al., 2014), multiple measures will be needed in order to quantify aspects of the complex information security construct (Vaughn/Henning/Siraj, 2003). Therefore, most of the standards and best practices currently in place describe multiple metrics needed to quantify certain aspects of information security. These standards and best practices include the ISO/IEC 27000 series with the ISO/IEC 27004 document (ISO/IEC, 2009) and the NIST 800 series with the special publication NIST SP 800-55r1 (NIST, 2008) to mention only two.

These standards have different areas of focus. While the ISO/IEC 27000 covers the information security management perspective, the NIST 800 series deals with a more technical view. The different perspectives are derived from the shift in responsibility from the technical information security employees to management (Diesch/Pfaff/Krcmar, 2020). Management has other questions than technical employees have. These include questions like whether the security is better this year, what management is getting for their security dollars or even how to compare their security to that of their peers (Geer/

Hoo/Jaquith, 2003). These questions must be answered not only by information security experts who have become managers but also by managers with less security knowledge. These managers are often located in small- and medium-sized businesses and came from other areas of expertise. Now they have to deal with issues involving complex information security and be responsible for it. To answer the management questions, rigorous metrics need to be defined and linked to the organization‘s management goals in order to support management decisions.

There are various information security metrics and frameworks in place for management. However, there is a gap in the connection between the technical security metrics and management´s goals. Information security managers tend to develop metrics with a top-down approach based on international standards, but they do not consider the realities of daily work (Hedström et al., 2011). Also, many security managers make decisions based on their experience, judgment and best knowledge. The reason for this is that managers do not have effective metrics in place, that security is complex and sensitive, and managers sometimes do not have enough historical data (Chai/Kim/Rao, 2011). Recent research articles have mentioned the gap that exists because of security metrics that are not connected to existing information security models or are not aligned to the management goals and strategic objectives of information security management (Bayuk/Mostashari, 2013; Collier et al., 2016; Pendleton et al., 2017; Azuwa/Sahib/Shamsuddin, 2017; Diesch/Pfaff/Krcmar, 2018).

This paper investigates the question of how information security metrics characterize and quantifies certain aspects of management success factors in the information security area. For this purpose, a literature analysis was conducted to obtain information security metrics. The next step was to use 12 management success factors (Diesch/Pfaff/Krcmar, 2020) as goals to conduct a Goal-Question-Metric approach in conjunction with the previously obtained information security metrics. This methodology was suggested by Rudolph/Schwarz (2012) which also stated the given gap and conclude, that this should “lead to a more goal-oriented strategy for deriving metrics that answers relevant questions and met predefined security goals”. The result is a list of metrics organized in clusters by questions and overall information security management goals. To the best knowledge of the authors, this is the first time information security metrics and information security management goals have been mapped this way. This research also includes a detailed description of what these metrics measure from the management perspective.

The remainder of this paper is structured as follows. Section 6.2 discusses the background and related work as well as the prerequisites for this paper. Section 6.3 outlines the methodology used to obtain the results. The results with the clustered information security metrics, the linkage to the management goals and a detailed description is given in Section 6.4. Section 6.5 critically discusses the results and contains suggestions for future research. The paper closes with a conclusion of the entirety of the work in Section 6.6.

6.2 Background and Related Work

A discussion of the link between information security metrics and the information security management goals includes the background of both worlds. Thus, Section 6.2.1 outlines the information security metrics with their different research areas and their focus in the past. Also, a definition of the terms is given within this section. In Section 6.2.2, an introduction to the current standards and best practices in information security management is included along with management success factors defined in the literature.

6.2.1 Information Security Metrics

The terms metric and measure are mostly used as synonyms in both practice and the literature. Also, the term metric does have different definitions depending on the subject area, the authors' preference, or the context in which they are being used. Azuwa/ Sahib/Shamsuddin (2017) reveals six different definitions of the term metric and measurement. This work differentiates the meaning of metrics and the measurement according to Pendleton et al. (2017). The authors noted that *"metric refers to assigning a value to an object while measurement is the process of estimating attributes of an object"* (Pendleton et al., 2017). In order to clarify the meaning of metrics, the following definition by Verendel (2009) is used in this research: *"A metric assigns data onto some kind of scale in order to correctly represent some security attribute of a system under consideration"* (Verendel, 2009).

Information security metrics are well discussed in existing research. Articles deal with the development of metrics (Zalewski et al., 2014; Mazur/Ksiezopolski/Kotulski, 2015; Collier et al., 2016; Young et al., 2016), taxonomies (Vaughn/Henning/Siraj, 2003; Purboyo/ Rahardjo/Kuspriyanto, 2011; Pendleton et al., 2017), usefulness of individual metrics (Bayuk, 2013; Savola, 2013) and their visualization (Savola/Heinonen, 2011). This underlines the statement that the "development of metrics that are valuable for assessing security and decision making is an important element of efficient counteractions to cyber threats" (Doynikova/Fedorchenko/Kotenko, 2019). However, as multiple authors have pointed out, there is a lack of a link between information security metrics and management goals (Bayuk/Mostashari, 2013; Collier et al., 2016; Pendleton et al., 2017; Azuwa/ Sahib/Shamsuddin, 2017; Diesch/Pfaff/Krcmar, 2018).

6.2.2 Information Security Management

Information security management is currently based on international standards and best practices. The ISO/IEC 27000 series is one of the most used standards and defines an Information Security Management System (ISMS). The ISMS is based on risk assessment and the individual risk acceptance level of an organization. "It is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security to achieve business objectives" (ISO/IEC, 2018). Besides the ISO/IEC 27000, there are other well-known frameworks and best practices like the NIST 800 series, COBIT, ISF, and NIST. Not all of them deal exclusively with information security management but they all do at least deal with parts of it. These documents define certain metrics for measuring the effectiveness of the ISMS. However, these metrics do not completely cover the minimum security requirements (NIST, 2008), and they struggle in structure and clarity as a recent study of McKinsey & Company pointed out (Boehm et al., 2018).

Soomro/Shah/Ahmed (2016) introduced a literature review on information security management and concluded that a holistic view on information security is missing in the literature. Based on this argumentation, Diesch/Pfaff/Krcmar (2020) developed a comprehensive model of management success factors for information security decision-makers based on standards, a state-of-the-art literature analysis, and an expert interview series. The model proposes 12 management success factors that have to be taken into account when making information-security-related decisions and deriving corrective actions. These factors are access control, awareness, infrastructure, vulnerability, physical security, CIA triad, continuity, risk, compliance & policy, security management, organizational factors, and resources. The first five factors are defined as key security indicators and the root cause of information security management decisions. As suggested within this article, these management success factors serve as management goals for this research. These categories were used because no other comprehensive model or theory was present in the literature - to the best of the authors knowledge.

6.3 Methodology

This section describes the methodology used to define metrics within current literature (Section 6.3.1). It also describe the Goal-Question-Metric approach to link the metrics to management success factors (Section 6.3.2).

6.3.1 Literature Analysis

The literature analysis has the goal to define metrics used in practice for describing aspects of information security. To reproduce the process of getting literature sources, the method of Webster/Watson (2002) was used. To obtain the most relevant literature in the search process, a keyword search was performed within academic databases. The searched databases were ScienceDirect, OpacPlus, and Google Scholar. OpacPlus is a wrapper that encompasses multiple databases like Scopus, Elsevier, IEEE Xplore, and Wiley to mention just a few. The search within Google Scholar was limited to the first 100 articles because the most relevant sources always appear on the first page (Silic/Back, 2014). The search string that was used to get the initial list of articles was:

```
(information OR cyber)
AND security
AND (metrics OR indicators OR measures)
```

Listing 6.1: *Literature search string*

The search was conducted by searching within the title, abstract, and keyword fields. The next step in the search process was to filter the number of articles according to the relevant articles by topic based on the title and abstract without duplicates. Finally, the articles were analyzed by searching for metrics. Articles that do not introduce metrics to measure an aspect of information security was excluded. All the steps and the number of articles within these steps are shown in table 6.2. In addition to the database search, the standards

ISO/IEC 27004 (ISO/IEC, 2009) and NIST SP 800-55 (NIST, 2008) were included in the literature analysis. The 45 resulting articles in the reduction step were analyzed by the first two steps of the "open-axial-selective" approach (Corbin/Strauss, 1990), which is not just the definition of clusters to a whole article but is about assigning first-order-codes to the content of the articles. The resulting metrics were first-order-codes. The second step is to combine synonyms and their meanings into second-order-codes. These are the result metrics for the step described in the following section 6.3.2. With this approach, metrics are included that are part of standards and best practices or are introduced by academic literature to measure aspects of information security.

Data source	**Hits**	**Reduction**	**Relevant**
OpacPlus	132	25	15
ScienceDirect	489	12	4
Google Scholar	100	6	5
Standards		2	2
Total	**721**	**45**	**26**

Table 6.2: *Literature search process*

6.3.2 The Goal-Question-Metric Approach

The Goal-Question-Metric approach (Basili/Weiss, 1984) is the most known and accepted method to develop goal-oriented metrics. One requirement for metrics is, that they should be goal-oriented by definition. Therefore, the last step of the previously stated "open-axial-selective" approach, which would be clustering the metrics by their meanings, is replaced. A clustering from bottom to top would result in metric-oriented clusters. Instead, a top-down approach from management success factors to metrics was used to cluster the metrics defined in the previous step. First, the 12 given management success factors (section 6.2.2) were used as goals for management. Second, questions were developed to explain aspects of each given goal. Last, the given metrics were assigned to the questions in order to quantify aspects of the goals. Metrics that could not be assigned in order to answer a given question were considered to be not goal-oriented.

6.4 Metrics and their Link to Management Goals

Each management success factor (Diesch/Pfaff/Krcmar, 2020) was given numerous questions that were derived from different standards and the problems described in the literature. The questions not only result from the literature analyzed but also from the clustering of the different metrics. The Goal-Question-Metric approach resulted in 50 questions that describe aspects of the 12 management success factors. The analysis of the 45 scientific articles of which 26 articles described different security metrics resulted in 322 metrics as first-order-codes. The linkage stage - included the elimination of duplicates - resulted in 195 metrics linked to the questions and, therefore, to the management goals.

The following subsections describe each factor with their related questions and metrics as well as how they quantify the given information security management goal. The metrics include several symbols. Table 6.3 show the meaning of each symbol with an example.

Symbol	Meaning	Example
%	Percent	% user accounts in compliance
Σ	Sum of	Σ admin violations
Ø	Average	Ø attack path death

Table 6.3: *Symbols used for information security metrics*

6.4.1 Access Control

The goal of **Access Control** is the regulation and minimization of access to applications, data, and infrastructure. The main challenges are off- and on-boarding processes and rules like "bring your own device" (Diesch/Pfaff/Krcmar, 2020) which increases the difficulty to manage access control.

Table 6.4 shows the related questions and the consolidated metrics from literature. Three main areas are important for organizations. First, the user accounts which are present in the infrastructure have to be compliant with given rules. Second, the users with extended rights on systems have to be monitored, because the misuse or corruption of these identities can cause great harm which results in an increased risk for the organization. The last area of interest are indicators of how strong the protection is. This area includes multiple metrics that count violations related to access control which indicates weak protection as well as possibilities to test the access control protection without having a violation. For example, the average password crack time indicates whether the passwords of identities are strongly protected against these types of attacks. All percentages and averages are based on the underlying number of available constructs described within the metric. The "% password matches minimum requirements" is calculated as $\frac{\Sigma\, Passwords\, match\, minimum\, requirements}{\Sigma\, Passwords}$.

Question	Metric
Are user accounts compliant?	% user accounts in compliance (Brotby, 2009)
Which users have admin rights?	Σ users with admin password or superuser or root privileges (Torres et al., 2006; Boyer/McQueen, 2007; NIST, 2008)
How strong is the access protected?	Σ unauthorized access/intrusion successes (Clark/Dawkins/Hate, 2005; Ravenel, 2006; NIST, 2008; Brotby, 2009; Hajdarevic/Allen, 2013), Σ strong credential keys (Boyer/McQueen, 2007), Σ failed logon attempts (Ravenel, 2006; Brotby, 2009), Σ logon violations (Kovacich, 1997), Ø password crack time (Herrera, 2005; Boyer/McQueen, 2008; ISO/IEC, 2009), Σ attempts to change security settings (Hajdarevic/Allen, 2013), % password matches minimum requirements (ISO/IEC, 2009; Radianti/Gjøsæter, 2017), % optional two factor authentication (Radianti/Gjøsæter, 2017)

Table 6.4: *Metrics to quantify access control*

6.4.2 Awareness

Awareness contains all activities and countermeasures to aware employees, managers and all people about information security issues and can not be treated by technical solutions. Metrics within this area deal with awareness training, awareness violations, and business management. To give an overview of information security awareness, the information security department or management must have an overview of the current users or employees within the organization. This leads to metrics like "Σ users" that are not related to information security in the first place but have to be monitored in order to calculate percentages out of it. Also, all departments of an organization should be involved in the information security department in order to meet information security requirements. A major area of interest is the awareness training. This area is strongly represented in literature as well as measures to assess violations related to awareness policies. The most cited author within this area is Torres et al. (2006) which defines multiple metrics to measure information security awareness training. The related questions are shown in Table 6.5.

Question	Metric
Are all users known?	Σ users (Kovacich, 1997), % individuals screened before enter the organization (NIST, 2008)
Are departments involved in information security issues?	% departments represented in the security committee (Herrera, 2005)
Do employees violate against awareness policies?	Σ admin violations (Ravenel, 2006; Brotby, 2009), Σ unauthorized access to web sites/documents/files (Ravenel, 2006; Hajdarevic/Allen, 2013), Σ reasons for revocation (Kovacich, 1997), Ø of user population revoked (Kovacich, 1997), Σ personnel reprimanded or fired for security decisions/actions (Freund, 2015)
Are employees trained and aware?	Σ best security practice incentives (Torres et al., 2006), Σ incidents reported per employee (Herrera, 2005; Torres et al., 2006; NIST, 2008), Ø training hours received per year (Torres et al., 2006), degree of awareness (survey) (Torres et al., 2006), % security budget spent on training (Torres et al., 2006), % satisfactory accomplishment per training activity (Torres et al., 2006; Andress/Leary, 2017), degree of organizational climate satisfaction (Torres et al., 2006), Ø users briefed (Kovacich, 1997), % managers with a NDA (Herrera, 2005), Σ employees with exclusive dedication to information security (Herrera, 2005), % managers with information security certification (Herrera, 2005; NIST, 2008), % personnel with security training (to their specific responsibilities) (Freund, 2015; Andress/Leary, 2017; ISO/IEC, 2009; NIST, 2008)

Table 6.5: *Metrics to quantify awareness*

6.4.3 Infrastructure

The **Infrastructure** is in contrast to vulnerabilities about the hardening of systems and all the components of the infrastructure. It is not just about hardening but also about knowledge of the infrastructure, its components, and also what attacks can occur within it. Table 6.6 shows the different areas of interest. The most crucial part is the questions about the knowledge of the current infrastructure of an organization. If an infrastructure component is not known or not managed by the security department, it has to be considered as not protected. The overview of the configuration state, the available communication channels as well as which components are monitored is asked to give an idea of possible attack vectors to the given infrastructure. Even if there are no official vulnerabilities reported to the current versions, accessible communication channels, and patch states there is the possibility of compromise through the given attack vector. The base to calculate percentages as well as averages is the number of systems within the infrastructure and therefore is also a metric within the question if all components are known. In practice, the term system has to be defined to set the scope of measurement and gain common acceptance.

Question	Metric
Are all infrastructure components known?	Σ systems (Black/Scarfone/Souppaya, 2008; Ryan/Ryan, 2008), Σ critical assets (Torres et al., 2006; Sun et al., 2011; Kotenko/Doynikova, 2013), Σ critical areas (Torres et al., 2006), Σ applications (Sun et al., 2011; Kotenko/Doynikova, 2013), % asset visibility (Black/Scarfone/Souppaya, 2008; Ryan/Ryan, 2008; Freund, 2015)
Are all components configured according to the definition?	Σ configuration weaknesses (Clark/Dawkins/Hate, 2005), % secured configurations (Torres et al., 2006), Σ security evaluation deficiency (Boyer/McQueen, 2008), Σ misconfigured devices (Ravenel, 2006), Σ firewall devices with retrieved configuration (Bayuk, 2013), % system interfaces accepts only valid input (Bayuk, 2013)
Are there newer versions of components or their services available?	% available patches applied (Brotby, 2009; NIST, 2008), Σ devices requiring remediation (Ravenel, 2006), % total hosts that require remediation (Ravenel, 2006)
Are all documented components available?	% configuration available (Radianti/Gjøsæter, 2017), % assets with control reviews (Freund, 2015)
Are all communication channels known?	Σ external communication paths (Boyer/McQueen, 2007), Σ remote accesses and wireless devices (NIST, 2008; Torres et al., 2006), Σ access points (Boyer/McQueen, 2008)
Are all components protected against known attacks?	Σ detection mechanism deficiency (Boyer/McQueen, 2008), Σ pc/servers with antivirus installed (Herrera, 2005; Andress/Leary, 2017)
Are all components owned and monitored?	% information system assets with owners (Herrera, 2005), % log files monitored (Hajdarevic/Allen, 2013; ISO/IEC, 2009)

Table 6.6: *Metrics to quantify infrastructure security*

6.4.4 Vulnerabilities

The goal to minimize **Vulnerabilities** within organizations is one of the most important goals that information security managers have. Vulnerabilities are connected to all management activities because they cause risks in case of available threats and, therefore, loss when they are disregarded. Vulnerabilities are seen in practice as technical vulnerabilities. Consequently, this management success factor is bound to be technical in nature which leads to the technical metrics shown in Table 6.7. To measure existing vulnerabilities the infrastructure has to be known and monitored. If systems are not monitored and updated, these have to be considered as vulnerable to attacks. Not just the monitoring itself but also the testing of infrastructure components lead to an improvement of the current information security status. A typical drawback by measuring information security vulnerabilities is the fact, that there are vulnerabilities that are not publicly available. These called zero-day exploits have to be taken into account when dealing with vulnerability metrics. It could create the wrong impression of security for managers.

Question	Metric
Are all security patches up to date?	% available patches applied (NIST, 2008; Brotby, 2009), vulnerability exposure (Boyer/McQueen, 2007; Kotenko/Doynikova, 2013), Σ security evaluation deficiency (Boyer/McQueen, 2008)
Are all infrastructure components known?	see infrastructure
Are all components scanned for vulnerabilities?	% tested/assessed systems (Black/Scarfone/Souppaya, 2008; Torres et al., 2006; Andress/Leary, 2017), % secured areas (Torres et al., 2006), % withstand targeted pentest attacks (Bayuk, 2013)
Are all published vulnerabilities of the infrastructure known?	Σ known vulnerabilities (Clark/Dawkins/Hate, 2005; Ravenel, 2006; Nichols/Sudbury, 2006; Sun et al., 2011; Brotby, 2009; Boyer/McQueen, 2007; Boyer/McQueen, 2008; Chakraborty/Sengupta/Mazumdar, 2012; Kotenko/Doynikova, 2013; Bayuk, 2013; Almasizadeh/Azgomi, 2013; NIST, 2008; ISO/IEC, 2009), Ø vulnerabilities per system (Boyer/McQueen, 2007), % systems without severe vulnerabilities (Kotenko/Doynikova, 2013)

Table 6.7: *Metrics to quantify vulnerabilities*

6.4.5 Physical Security

The physical protection of buildings, infrastructure, offices, and other hardware is a special topic in conjunction with information security. **Physical security** is related to information security but mainly it is not part of the organization‘s information security department but of corporate security (Diesch/Pfaff/Krcmar, 2020). Therefore, Table 6.8 include just metrics related to the physical protection of infrastructure components which are critical for the business of an organization as well as the underlying number of critical systems. The number of resulting metrics also represent their presence in literature.

Question	Metric
Are critical components physically protected?	% critical equipment with adequate physical protection (Torres et al., 2006; ISO/IEC, 2009; NIST, 2008), host criticality (Sun et al., 2011; Kotenko/Doynikova, 2013)

Table 6.8: *Metrics to quantify physical security*

6.4.6 CIA Triad

The **confidentiality, integrity, and availability (CIA)** are the "protection goals" of information security but are called in practice as a theoretical construct from research. When it comes to decision-making, practice shows that management depends less on these protection goals than expected (Diesch/Pfaff/Krcmar, 2020). Nevertheless, the goal to protect confidentiality, integrity, and availability is very important in terms of communication and the understanding of certain countermeasures. Also, risks can be explained more easily when explaining the impact based on the CIA construct. The literature has shown the difficulty of measuring these attributes but provides metrics for consideration. These metrics are summarized in Table 6.9. It is also visualized in the low amount of metrics conducted out of the literature. Metrics can be used to quantify the availability of networks, documents, and systems. Aspects of confidentiality and integrity are just be measured indirectly by providing encrypted communications and perform tests which, in the case of outliers, indicate possible violations such as transmission exposure.

Question	Metric
Are all documented components available?	Ø service availability time (Clark/Dawkins/Hate, 2005; Jonsson/ Pirzadeh, 2011), % network reachability (Sun et al., 2011), % systems availability (Torres et al., 2006)
Are communication paths encrypted?	data transmission exposure (Boyer/McQueen, 2008), Σ unauthorized information disclosures (Ravenel, 2006), % encrypted communication Radianti/Gjøsæter (2017), % media that passes sanitization procedures (NIST, 2008)

Table 6.9: *Metrics to quantify CIA*

6.4.7 Continuity

Continuity is in contrast to the availability, not just the availability of systems but the continuous delivery of the intended outcome. This includes business continuity as well as systems continuity and is a major goal of information security and business management. The most questions arise in case of a malfunction or disaster in which the system must be recovered as quickly as possible. The questions and metrics present in literature and shown in Table 6.10 is related to the possibility and the test to recover systems and services as well as a buffer of available resources.

6.4.8 Risk

Information security management standards are mostly based on a risk management approach. The assessment of available **Risks**, their classification and the development of countermeasures are therefore the main activities for information security managers. Minimizing risks according to the risk acceptance level is, therefore, an important goal for information security managers. The metrics and questions arising within this section are strongly related to the risk definition. Risks are present if an asset has a vulnerability and a possible threat. To quantify the risks, the impact and probability of occurrence have to be considered. Each organization has its risk acceptance and risk appetite. The metrics in Table 6.11 are present in the literature and quantify the different aspects described.

Question	Metric
Are backups for components in place?	Σ data recovery testing (Torres et al., 2006), Σ protected files (Torres et al., 2006)
Is it possible to recover a malfunction service?	Ø mean-time-to-repair systems (Boyer/McQueen, 2007; Jonsson/Pirzadeh, 2011), Ø business critical data recovery time (Torres et al., 2006), Ø critical data recording date (Torres et al., 2006)
Do activities impact continuity?	patch risk (Sun et al., 2011), Ø systems mean-time-to-failure (Jonsson/Pirzadeh, 2011), Ø mean time to catastrophic failure (Jonsson/Pirzadeh, 2011), Σ remaining storage capacity (Boyer/McQueen, 2007; Boyer/McQueen, 2008; Brotby, 2009), Σ point solutions (Torres et al., 2006)

Table 6.10: *Metrics to quantify continuity*

6.4.9 Compliance & Policies

Compliance & Policies come from different sources like the security management of an organization, laws, regulations, and other requirements. The goal of the management is to comply with these regulations in order to achieve certifications or not violate laws. The challenge is that a fully compliant organization may not mean a fully secure organization (Diesch/Pfaff/Krcmar, 2020). These written rules have to be monitored in order to evaluate their effectiveness. If no policies are in place, it is difficult to push regulations through when violating them. Therefore, the first question within Table 6.12 refers to the existence of policies. Policy violations and the opposite, the compliance to policies, are also measured by literature. An important topic in literature is, that policies are backed up by the management.

6.4.10 Resources

Resources does not just mean financial budgets but also includes an appropriate number of skilled people and the appropriate time to perform the necessary tasks. Thus, the effectiveness of resource investment and employee management, as well as the availability of time for projects, is shown in Table 6.13. The problem when quantifying the effectiveness of security investments is, that they are not easy to understand and to use. To calculate the return on security investment (ROSI), it is necessary to assume the loss expectancy in case of corruption, the mitigation ratio for a proposed solution as well as the cost of the solution. These preconditions alone are difficult to measure and quantify. However, if this process is carried out carefully, not only the information security management but also the business will understand the value of information security.

6.4.11 Security Management

Information **Security Management** has the goal of developing, implementing and improving information security within organizations. This goal can be achieved by implementing processes that are described in multiple standards and best practices like ISO/IEC 27000 (ISO/IEC, 2018), NIST 800 (NIST, 2018b), ITIL, and COBIT. To quantify aspects of the effectiveness of the information security management, questions have

Question	Metric
Are there vulnerabilities?	see vulnerabilities
Are exploitable threats available?	Ø CVSS score (Sun et al., 2011), processor or bandwidth utilization (Brotby, 2009; Freund, 2015), Σ identified potential threats (Brotby, 2009; Torres et al., 2006; Chakraborty/Sengupta/Mazumdar, 2012; Freund, 2015)
Are all components of the infrastructure related to a risk?	Ø computer/host criticality (location, application, role) (Kotenko/Doynikova, 2013; Sun et al., 2011), % software and hardware classified (Torres et al., 2006), % assets with completed risk assessment (Torres et al., 2006; Drugescu/Etges, 2006; Freund, 2015; Andress/Leary, 2017), % risk assessment automatization (Torres et al., 2006)
What is the probability?	% probability of compromise (Brotby, 2009), Ø attack path death (Boyer/McQueen, 2008), Σ attack surfaces (Almasizadeh/Azgomi, 2013)
What is the impact in case of occurrence?	Σ worst case loss (Ryan/Ryan, 2008; Boyer/McQueen, 2007; Boyer/McQueen, 2008), Σ business value (Kotenko/Doynikova, 2013)
What is the current risk level?	Σ value at risk (Brotby, 2009), Ø level of risk by area (Torres et al., 2006), risk level (Clark/Dawkins/Hate, 2005; Ryan/Ryan, 2008; Kotenko/Doynikova, 2013; Freund, 2015), risk exposure (Kotenko/Doynikova, 2013), downstream risk (Kotenko/Doynikova, 2013), Σ it risk (Drugescu/Etges, 2006; Ravenel, 2006)
What is the accepted risk level?	risk acceptance level Freund (2015), Σ risks accepted (Freund, 2015), Σ high risks accepted (Freund, 2015)

Table 6.11: *Metrics to quantify risks*

to be answered regarding the processes of the information security management program. The area of information security management processes is well described in scientific literature as well as in current standards and best practices. The sanitation of available metrics from this area shows, that the metrics are quantifying the effectiveness of typical information security processes or the ability to cover and detect attack attempts. The typical metrics contain a time component or a percentage processing of existing tasks. However, operational security does not quantify aspects of information security but the ability of an organization to detect, plan, and process information security-related tasks in an effective way. This is important for the management to continuously improve and maintain the security status of the organization. Also, Lee/Geng/Raghunathan (2016) reveals, that a higher security standard does not necessarily lead to a higher security level. Table 6.14 shows the overview of the related questions with the metrics from the literature. There are multiple examples illustrates this. The number of viruses detected and isolated shows that viruses can be detected and the ability of the security staff to isolate them. This indicator does not cover any other aspect but the effectiveness of the security operations department. Nevertheless, if information security operations is not in place, it could be argued, that the security of an organization is not protected at all. Thus, information security operations have to be monitored and also improved in order to improve the information security status of an organization in a structured way. Another example is the average known vulnerability days which indicates how long a known vulnerability exists. The metric measure the effectiveness of vulnerability management but

Question	Metric
Are policies in place?	Σ security policies/controls (Torres et al., 2006; Ryan/Ryan, 2008), % policies and procedures into the design phase (Torres et al., 2006)
Are there policy violations?	% user accounts in compliance (Brotby, 2009), maturity level of current controls (Torres et al., 2006),, Σ policy violations (Ravenel, 2006)
Are policies accepted by the management?	% policies and procedures documented and approved (Torres et al., 2006), % strategy robustness (Torres et al., 2006), % managers involved in the information security policy definition/evaluation/review (Herrera, 2005)
Are all rules fulfilled?	% compliance (Clark/Dawkins/Hate, 2005; Torres et al., 2006; Brotby, 2009; Ryan/Ryan, 2008), Σ systems certified (Ryan/Ryan, 2008), Σ audits outsourced/internal (Torres et al., 2006; Bayuk, 2013; Freund, 2015; NIST, 2008), % fulfilled regulations (Torres et al., 2006), % security requirements addressed in third party agreements (ISO/IEC, 2009)

Table 6.12: *Metrics to quantify compliance*

Question	Metric
Are projects in time?	Ø project delays (Torres et al., 2006)
Is budget enough and effectively used?	ROSI (Brotby, 2009; Torres et al., 2006; Böhme, 2010), security investment benefit (Ryan/Ryan, 2008), security budget segregation/evolution (Torres et al., 2006), Σ cost-benefit (Kotenko/ Doynikova, 2013; Andress/Leary, 2017), information security budget in current year (Herrera, 2005), cost and effort of patch process (Nichols/Sudbury, 2006), % budget devoted to IS (NIST, 2008)
Is there enough qualified staff?	% qualified IS staff (Torres et al., 2006; Herrera, 2005), % responsibility sharing (Torres et al., 2006; NIST, 2008), % in house specialized staff dedicated to assessment of info-sec activities (Torres et al., 2006)

Table 6.13: *Metrics to quantify resources*

not the actual state of vulnerabilities within the organization. Both aspects are important but measure different things.

Question	Metric
Is the top management involved?	% suggested procedures approved (Torres et al., 2006), % policies and procedures documented and approved (Torres et al., 2006), % strategy robustness (Torres et al., 2006), Σ downstream and upstream info-sec communication (meetings to top level management) (Torres et al., 2006), Σ managers attending the security committee meetings (Herrera, 2005), % business initiatives supported by information security (Andress/Leary, 2017), % agreements with information security clauses (Andress/Leary, 2017)

Which attacks and problems can be detected by the security management?	Σ incidents (Torres et al., 2006; Herrera, 2005; Hajdarevic/Allen, 2013; Drugescu/Etges, 2006; ISO/IEC, 2009; NIST, 2008), Σ packets dropped by firewall (Brotby, 2009), Σ viruses detected in user files/e-mails/websites (Brotby, 2009; Ravenel, 2006), Σ intrusions detected/attempts (Brotby, 2009; Ravenel, 2006), Σ spam (not) detected/filtered/false-positive (Ravenel, 2006), Σ firewall false negative (Bayuk, 2013)
What external partners have to be managed?	Σ contracts with third parties (ISO/IEC, 2009; Torres et al., 2006), % outsourced information security processes (Torres et al., 2006)
How effective are problems handled?	Ø mean-time-to-repair systems (Boyer/McQueen, 2007; Jonsson/Pirzadeh, 2011), Σ viruses detected and isolated (Brotby, 2009; Torres et al., 2006; Ravenel, 2006), % audit items closed (Brotby, 2009; Drugescu/Etges, 2006), time between vulnerability discovery and repair (Boyer/McQueen, 2007), Ø known vulnerability days (Boyer/McQueen, 2008), Ø time to respond to incidents (Torres et al., 2006), % incidents stopped per month (Torres et al., 2006; Andress/Leary, 2017), % nonconformity aspects fixed (Torres et al., 2006), certification status (hours needed to achieve certification) (Torres et al., 2006), % audit findings closed, (Drugescu/Etges, 2006), min/max/mean time to correct a variance (Freund, 2015)
How effective are other security related processes?	Ø hours dedicated to policies and procedures design/implementation/reviews/updated (Torres et al., 2006), % high-impact incidents on processes not contemplated in previous risk assessments (Torres et al., 2006), % internal audits accomplished (Bayuk, 2013), Ø attendees per brief (Kovacich, 1997), Ø average system approval time (Kovacich, 1997), Σ actualization's distributed in the last two weeks (Herrera, 2005), Σ corrective actions taken after specific event (Hajdarevic/Allen, 2013; ISO/IEC, 2009), Σ newly identified it risks (Drugescu/Etges, 2006), Σ remediations applied by time and type (Ravenel, 2006), Ø time to patch systems (Nichols/Sudbury, 2006), Σ reviews by third parties (ISO/IEC, 2009)
Are changes handled through security management?	Σ changes in compliance (Clark/Dawkins/Hate, 2005; Boyer/McQueen, 2008; Herrera, 2005; NIST, 2008), Σ system configuration changes(Boyer/McQueen, 2007), Σ architecture changes (Torres et al., 2006), min/max/mean time to discover a configuration variance (Freund, 2015)

Are countermeasures/actions planned and implemented/done?	Σ successful implementations of security procedures (Ryan/Ryan, 2008), evolution of information security plan of action (Torres et al., 2006), % daily monitored processes (Torres et al., 2006), % monthly systems performance and assurance scheduled activities (Torres et al., 2006; NIST, 2008), % maintenance processes executed (Torres et al., 2006), % countermeasures implemented (Torres et al., 2006), Ø risk assessment review time (Torres et al., 2006), Σ managers monitored (Herrera, 2005), % risk management actions planned/approved/rejected Drugescu/Etges (2006), Σ privacy risk monitoring activities and reports (Drugescu/Etges, 2006), Σ policy exception reviews (Freund, 2015), frequency of control reviews (Freund, 2015), maintenance delay per event (NIST, 2008; ISO/IEC, 2009)

Table 6.14: *Metrics to quantify security management*

6.4.12 Organizational Factors

Organizational Factors must be considered by making information security-related decisions but can not be converted into a goal for the information security manager (Diesch/Pfaff/Krcmar, 2020). This factor might have an impact on whether it is possible to push policies and countermeasures through an organization or have an impact on the risk appetite as well as the possibility to hire their own staff related to information security. However, an optimal organizational size or structure is not achievable by the information security management. There are no metrics described in the literature that quantify aspects of this factor.

6.5 Discussion and Future Research

This study synthesizes available information security metrics and links them to management success factors. To achieve this link, each management success factor was extended by questions with the help of the Goal-Question-Metric approach. Each question explains a different aspect of the related management success factor. Metrics from the literature, revealed with the help of a systematic literature review, were then assigned to one or more of the questions. Assigning these metrics leads to a clustering of available security metrics in the literature to management goals. That was asked by multiple authors in literature and requested by practitioners. This research enables security practitioners to look for specific metrics that can be used to quantify a specific goal and improve it over time. This opportunity is especially useful for small- and medium-sized businesses because they might not have the expertise to develop their own goals with specific metrics.

The distribution of metrics leads to the conjunction that there might be a set of core metrics that are required because they measure aspects of multiple goals at once. This explains the overlap of some of the metrics. An example is “known systems” which is important for understanding the infrastructure as well as it is for recognizing vulnerabilities. This turns out to be the case because an unknown and therefore not monitored system has to be defined as vulnerable. If an organization wants to establish metrics, these metrics would have the biggest impact on the organization‘s information security.

Clustering and calculation of the metrics show that some metrics are dependent on others. The best example is the risk goal. This goal can be reached by quantifying the goal of minimizing vulnerabilities as well as by knowing the infrastructure and, therefore, the threat landscape. Also, possible risks can occur from all key security indicators as shown in a previous study Diesch/Pfaff/Krcmar (2020). The assigned metrics also show these dependencies through their calculation. This means that some metrics must be implemented before others can be applied and, thus, are their prerequisites. Practitioners and researchers also have to consider the prerequisites to collect the different data that are needed to instantiate the metrics. There, the cost and effort of collecting these data have to be weighted. Also, managers with less information security background are able to look over the different aspects and easily assess the needed tasks to protect their organization. An example would be, if a metric like Σ known systems is suggested, an organization has to think about implementing a configuration management database or asset system in order to quantify this metric. Also, an infrastructure scanning tool, which reveals hidden systems is needed to distinguish between known and unknown systems. This result in the need for thinking about the availability of data, their usefulness, and accuracy.

Multiple authors have mentioned the same metrics but have articulated them in different wording, scales or contexts. There were also authors that mentioned multiple metrics in the same article, but they had the same meaning although they had different names. This makes it clear that there is still no common understanding of information security metrics in the literature. This study can help to determine such an understanding.

Previous work deals with multiple suggestions about specific metrics. These metrics are helpful to measure certain aspects of information security. This work combines the information security management perspective with the technical information security metrics view to link them together so that a practitioner and a researcher have the ability to understand each other‘s needs and background. The research of information security metrics was extended by clustering them to management success factors as well as the other way around.

Each study has its limitations and creates opportunities for further research. The literature survey was rigorously conducted using the proposed methodology but is limited to the asked databases and, thus, might not contain each relevant article. Also, the filtering process as well as the analysis and assignment steps were done to the best of the authors‘ knowledge but could include subjective meanings of the authors. An empirical study can be conducted to evaluate the proposed metric assignment as well as the usability and understandability of the metrics. The information security management has the opportunity to choose or implement all the proposed metrics, but the number of them is very large which could lead to information overload effects. Therefore, future research could investigate combining and aggregating the different metrics from the individual goals to develop a key indicator for each goal that could then be presented to the information security management. Such an information security management dashboard was asked by different experts in the field (Diesch/Pfaff/Krcmar, 2020) and is requested in recent research articles (Maier et al., 2017; Al-Darwish/Choe, 2019; Tewamba et al., 2019). The proposed systematization of metrics from the literature can serve as the basis for such dashboard developments as well as research in the field of quantifying and developing key security indicators. A further research possibility could be the design, architecture, and development of a solution to automatically collect the necessary data for security metrics from an organization. Also, a question remains if all metrics are really necessary and useful to measure the actual information security status of an organization. An example would be spending hours on training and if the awareness increases with more training hours. Especially if the training itself is not effective. Other authors criticize metrics within standards and best practices regarding their objectives. They measure the effective implementation of countermeasures and not the actual information security status of an organization or if the countermeasures itself are effective (Bayuk, 2013). This applies mainly to metrics within the "security management" cluster within this article. It can be argued that these metrics are not useful for measuring the actual information security status but the effective implementation of processes and countermeasures. The detailed discussion of each metric depends on the context and is out of scope of this research article. Therefore, future research should empirically test the proposed metrics in order to evaluate their meaningfulness and usability in measuring the actual information security status of an organization.

6.6 Conclusion

Information security metrics are the most common method to measure the effectiveness of information security countermeasures and concerns in organizations. There are many metrics described in the literature. However, they are not related to security management goals. Therefore, this study investigates how information security metrics from the literature can be linked to security management goals.

To answer the research question, a state-of-the-art literature analysis was conducted to define metrics. After that, 12 management success factors were defined as management goals. The Goal-Question-Metric approach was used to specify different aspects of the goals. Finally, the metrics were assigned to the developed questions in order to cluster the metrics to the information security management goals.

The results combined the two research streams of information security metrics and information security management objectives. Therefore, it helps to understand what the metrics quantify from the management perspective and the other way around. The results can be used to further develop key indicators, conduct empirical studies, and investigate in the research of possible dashboards for the information security management. Also, the research can provide an opportunity to design a technical information security assessment solution.

Part B2

Working Papers

7 A Method to Aggregate Information Security Metrics

Title	Reducing Complexity - A Method to Aggregate Security Metrics
Authors	Diesch, Rainer[1] (rainer.diesch@tum.de) Pfaff, Matthias[1] (pfaff@fortiss.org) Krcmar, Helmut[1] (helmut.krcmar@tum.de) [1]Technical University of Munich (TUM), Boltzmannstraße 3, 85748 Garching, Germany
Type	Journal
Outlet	Computers & Security
Publisher	Elsevier Inc.[3]
Ranking	ERA 2010[4]: B Impact Factor 2019[5]: 3.579 Computers & Security is recommended by the Senior Scholars' Basket of Journals – AIS Special Interest Group Security (SEC)[6]
Status	Submitted
How to Cite	-
Individual Contribution	Conceptualization, Methodology, Investigation, Data Curation, Writing - Original Draft, Writing - Review & Editing, Visualization

Table 7.1: *Bibliographic details for P4*

[3] https://www.elsevier.com/

[4] http://portal.core.edu.au/jnl-ranks/365/

[5] Clarivate Analytics Journal Citation Reports, https://jcr.clarivate.com/

[6] https://aisnet.org/page/SeniorScholarBasket

Reducing Complexity - A Method to Aggregate Security Metrics

Abstract: Information security metrics are the standard method to evaluate the effectiveness of information security countermeasures and derive decisions. A security manager of an organization can choose from more than 900 of them. This variety of metrics leads to security management reports with a lack of standardization, clarity, structure, and consistent real-time data. Therefore, this study uses a design science approach to develop a method to aggregate information security metrics. The result is evaluated with an instantiation which quantifies vulnerabilities, a simulation, and a semi-structured expert interview with 16 experts from practice. The study enables security and business management to develop useful key security indicators in a standardized way by reducing the negative effects of information asymmetry, information aggregation, and information overload.

7.1 Introduction

Information security remains one of the main issues for organizations because of the great losses in case of security breaches. The growing number of vulnerabilities, law restrictions and high expenses in case of a data breach or an information security incident are reasons for organizations to invest in information security (IBM Institute for Business Value, 2018). The (ICS)^2 Cybersecurity Workforce Study ((ICS)^2, 2018) reported 2.9 million open positions in the information security field. This strongly shows the need for security expertise in practice.

Various frameworks, standards and best practices (e.g. ISO/IEC 27000 (ISO/IEC, 2018), NIST Cybersecurity Framework) help organizations manage information security. An important part of these frameworks is information security monitoring and the validation of countermeasures and policies. To address the need for monitoring and evaluation, separate documents within the frameworks were developed. Examples are the NIST 800-55 (NIST, 2008) or ISO/IEC 27004 (ISO/IEC, 2009) which proposes a security metrics development method and suggest examples of metrics (e.g. "number of vulnerabilities", "number of security trained personnel", "number of security assessments conducted" (ISO/IEC, 2009)). Research articles in recent years deal with metric taxonomies (Pendleton et al., 2017; Purboyo/Rahardjo/Kuspriyanto, 2011; Verendel, 2009), metric development (Collier et al., 2016; Young et al., 2016; Mazur/Ksiezopolski/Kotulski, 2015), their usefulness (Holm/Afridi, 2015; Mermigas/Patsakis/Pirounias, 2013; Jafari et al., 2010), effectiveness of specific metrics (Coronado et al., 2009; Bayuk, 2013; Savola, 2013), and visualization (Savola/Heinonen, 2011). These information security metrics are very specific and, in most cases, technical in nature. Herrmann's book "A Complete Guide to Security and Privacy Metrics" (Herrmann, 2007) lists 900 different metrics which are considered to be appropriate for use in decision-making by practicing auditors, engineers, and managers. A survey of McKinsey & Company (Boehm et al., 2018) identified three problems with information security reports that information security and business managers face:

1. Multiple reports include far too many Key Performance Indicators (KPIs) regarding information security. They are poorly structured, inconsistent, and have too many details. This results in a **lack of structure** within reports.

2. A **lack of clarity** within reports was identified because they do not include an explanation of the indicators. They are not explaining the implications for the business level or their technical meaning in a way the management can understand. The reports struggle to explain the overall security level of the organization.

3. A **lack of consistent real-time data** means that different groups of the organization use different and sometimes conflicting information to report the indicators. This results in different descriptions and evaluations for similar aspects of information security. Therefore, a comparison of divisions or different organizations is not possible.

The three shortcomings above decrease the quality of decision-making, and therefore cause financial and reputation loss. Different authors of scientific literature also identified the shortcomings in research. Scientific literature deals with security metrics that are highly diverse. Authors criticized that widely accepted attempts are missing (Savola, 2009; Chai/Kim/Rao, 2011; Bayuk/Mostashari, 2013). The lack of clarity is confirmed by different authors who stated that the used metrics do not give managers the information they need to support decisions and articulate the value of security activities (Hayden, 2010; Jafari et al., 2010; Chai/Kim/Rao, 2011; Bayuk, 2013; Fenz et al., 2013; Azuwa/Sahib/Shamsuddin, 2017). The existing security metrics are not appropriate to compare them cross-organizationally Jafari et al. (2010); Mermigas/Patsakis/Pirounias (2013); Bayuk (2013). Various authors have explicitly identified the need for research in closing the gap between technical metrics and reports for information security and business managers to evaluate their mitigation approaches (Sowa/Gabriel, 2009; Leon/Saxena, 2010; Crossler/Belanger, 2012; Savola, 2013; Collier et al., 2016; Pendleton et al., 2017; Onibere/Ahmad/Maynard, 2017; Diesch/Pfaff/Krcmar, 2018). A method that captures the various existing information security metrics and aggregates them to quantify a security management goal could help to close the gap between the technical and the management view on the organizational information security. Also, Diesch/Pfaff/Krcmar (2020) showed that current approaches for developing key indicators are not goal oriented. Therefore, this study asks the research question: How can information security metrics be consolidated and prepared for the security management of an organization?

Using design science research (Hevner et al., 2004), this study develops a method to aggregate information security metrics into overall key security indicators with respect to the current problems that organizations face. To show the usefulness and practicality of the result, the paper includes an instantiation of this method. To further show that the result prerequisites have been met, a simulation and comparison with a current metric have been included. Finally, a semi-structured expert interview was conducted to evaluate the understandability, clarity, and usefulness as well as show additional advantages of the proposed result. Also, current practices from experts regarding information security metrics and further insights were explored and present in this research study.

The remainder of the article is structured as follows: A review of existing frameworks and techniques to develop, describe and present security metrics is shown in the following section. Section 7.3 explains the research approach for this article. This includes the design science approach used to develop the security metrics aggregation method (Section 7.3.1) as well as the methodology for the expert interview series (Section 7.3.2). The resulting information security metrics aggregation method is shown in Section 7.4 and contains the underlying requirements, an instantiation of this method as well as the evaluation with the help of a simulation and the expert interview result. A critical discussion, future research, and limitations is provided in Section 7.5. The article ends with a conclusion in Section 7.6.

7.2 Background and Related Work

The field of security metrics and thus security evaluation comes from the need to measure security (Dhillon/Backhouse, 2001). Previous work deals with techniques to help with securing systems. In the past, information security was a technical topic and the responsibility for the related issues within organizations lay with technical employees (Willison/Backhouse, 2006). Today, the responsibility is shifting to the top management of organizations (Soomro/Shah/Ahmed, 2016). Because of the shift from the technical to the management perspective, there are various approaches to deal with security metrics from both worlds which are discussed in research too. This article uses the term security metric as a "reflection of quantitative security attributes based on certain scales" (Pendleton et al., 2017). Security metrics refers to the assignment of "a value to an objective while the measurement is the process of estimating attributes of an object" (Pendleton et al., 2017). When it comes to management decisions, different theories deal with different aspects of decision making including the characteristics of the underlying information to make these decisions. The following subsections describe available security metric approaches in practice and literature as well as underlying theories.

7.2.1 Security Standards and Best Practices

Standards and best practices are commonly used by practitioners to implement information security within organizations (Siponen/Willison, 2009). The most common standard is the ISO/IEC 27000 series (ISO/IEC, 2018). The standard defines requirements and controls for an information security management system and uses a risk-based approach to deal with security issues. Security controls have to be continuously planned, implemented, reviewed and improved. The improvement is referenced within a stand-alone ISO/IEC 27004 (ISO/IEC, 2009) document which deals with information security measurement and metrics. This document is a guide for practitioners to develop and use metrics for measuring the effectiveness of the information security management system and the underlying controls. The measurement guide provides a detailed description of how to define metrics and gives certain examples of them. The metrics are mainly to measure the effectiveness of the information security management system but not the specific goals of the business for the information security of the underlying organization. Aggregated metrics called "derived measures and measurement functions" are also described. These aggregated metrics are defined as a metric of two or more metrics which are combined with a measurement function. This measurement function is a calculation.

An example measurement function could be "$Metric.1/Metric.2 * 100$". The aggregation, therefore, is a specific measurement function which combines different metrics to overall aggregated indicators based on calculations.

The National Institute of Standards and Technology published the NIST 800 series as a framework for computer security which also includes a "Performance Measurement Guide for Information Security". This special publication NIST 800-55 (NIST, 2008) provides a detailed description of measurements, best practices, taxonomies, a metrics development process and also the collection of necessary data for these metrics. The document series also proposes candidates of metrics. NIST 800 emphasizes that these metrics are neither complete nor address the minimum security requirements (NIST, 2008). An aggregation method or a reporting visualization is not provided.

Other standards and best practices are either highly technical (e.g. Common Criteria for Information Technology Security Evaluation (CCIB, 2017)) or treat information security from a highly abstract or governance perspective (e.g. COBIT (ISACA, 2012)). These documents do not describe methods to aggregate certain proposed metrics. The missing monitoring and review approaches are also identified by Höne/Eloff (2002). They reviewed and identified different elements and characteristics of six common security standards. The category "Monitoring and Review" is available just in one of the standards and best practices they reviewed. The standard BS7799 is the predecessor of the ISO/IEC 27000 series and includes a monitoring. This monitoring is described above within this section.

7.2.2 The Goal Question Metric Approach

There are certain available methods to develop metrics. An approach which is considered to be very successful in practice is the goal-based approach (Berander/Jönsson, 2006). Basili/Weiss (1984) introduces the best known of these: the GQM approach. GQM is a top-down approach to develop metrics that treats three levels of development. The conceptual level (Goal) consists of measurement goals regarding products, processes or resources. The operational level (Question) is a set of questions which characterizes and describes the goals. The quantitative level (Metric) is the definition of the metrics that are answering the questions of the previous level. This approach is widely used in practice and in the literature and is also further developed by other authors like Berander/ Jönsson (2006). The principle of the GQM approach is also used for various other topics like the security metrics taxonomy development (Savola, 2007). The GQM approach is announced to develop fewer yet meaningful metrics. The method does not provide the criteria that the metric is necessary for the goal or aggregate them back to the goal or to a management level. Thus, an aggregation of the metrics to key indicators for the management level is not provided by this approach. Besides the existing approaches, different research articles call for a more goal-oriented approach to generate more meaningful and useful metrics (Jafari et al., 2010; Leon/Saxena, 2010; Rudolph/Schwarz, 2012; Bayuk/ Mostashari, 2013; Collier et al., 2016). The gap between the state-of-the-art metrics and security-related goals are mentioned by different authors and is still a valid research gap (Collier et al., 2016; Pendleton et al., 2017; Diesch/Pfaff/Krcmar, 2018).

7.2.3 Attack Graph-Based Metrics

The concept of attack graphs was first proposed by Phillips/Swiler (1998) for network security testing. This concept was later generalized by Jha/Sheyner/Wing (2002) to not just provide network security testing. An attack graph is “a succinct representation of all paths through a system that end in a state where an intruder has successfully achieved his goal” (Jha/Sheyner/Wing, 2002). Historically, this approach is used for detection, defense, and forensic approaches. Different metrics based on attack graphs were developed to quantify the security state of a network, an application or other systems. Also, techniques to aggregate these metrics are applied by other authors. Idika/Bhargava (2012) proposed multiple aggregated metrics based on attack graphs like “shortest path metric”, “number of paths” and the “mean of path lengths metric”. A disadvantage of this method is the attack graph itself. The graphs are difficult to develop and complex in nature. Therefore, an attack graph might not be understandable for non-experts and also not comparable with other organizations or departments of an organization.

7.2.4 Security Metrics

Security metrics are discussed by multiple authors in the literature. A state-of-the-art literature review on security metrics and measurement was conducted by Diesch/Pfaff/Krcmar (2018). The articles are categorized in different areas of research which, in the case of security measurement, are: “development”, “taxonomy”, “security metrics”, “effectiveness” and “visualization”. The interesting part for this research - namely “security metrics” - describes a class of articles that deal with specific metrics and and their detailed evaluation or simulation. A standardized method to aggregate security metrics to higher levels of goal-oriented key security indicators is not provided in past research.

However, there are different approaches to develop, describe and specify security metrics as well as different security standards which describe security categories and their relationships in the literature, an approach to close the gap between technical security metrics and the goals of the security management are not present. Also, no current widely accepted information security evaluation framework exists as von Solms et al. (1994) already recognized in their work. Therefore, this study develops a method to aggregate well-described security metrics to goal-oriented key security indicators for the security management of an organization.

7.2.5 Decision Theory

Decision theory is derived from basic management science and theory. Because a major task of managers is to make decisions, the decision theory arises which focuses on the characteristics of how to make decisions (Koontz, 1980). Therefore, Polasky et al. (2011) defined decision theory as “a powerful tool for providing advice on which management alternative is optimal given the available information”. In other words: Decision theory is an approach that uses available information to make optimal decisions under uncertainty. The uncertainty is represented by assuming a set of possible states of a system with a dedicated probability for the occurrence (Koontz, 1980). Therefore, a manager has a set of actions to generate an outcome with a benefit. This benefit can be expressed in a common metric (Morgan/Henrion, 1992). One prerequisite to achieve a rational decision is the availability of possible alternatives and actions as well as a common understanding of the underlying problem. Also, many theories derive out of the availability of information and uncertainty. The relevant parts of the theories for this research are outlined in the following subsections.

7.2.5.1 Behavioral Decision Making

Behavioral decision making in literature deals with different decision making heuristics and how they perform (Csaszar/Eggers, 2013). The decision making is divided in literature into an interpersonal and a group behavioral approach. The interpersonal approach deals with the thesis that managing involves to get things done through people. This research deals with interpersonal relations and is oriented to individual psychology, motivations, and leadership. Group behavior is concentrated on people in groups. Research in this area concentrate therefore on sociology, anthropology, and social psychology (Koontz, 1980).

A major finding for this research is that several heuristics can perform in a similar matter than optimal decision rules (Csaszar/Eggers, 2013). These heuristics do not contain all available data or even internal parameters that point to decisions under uncertainty, under data asymmetry and data aggregation. These topics and their relation to this research are described in Section 7.2.5.2.

Vessey (1994) explained that the research of behavioral decision making also observed that decision-makers see quite minor tasks and environmental changes and adapt their strategy in response to them. This leads to the cost-benefit theory which says that decision-makers trade-off between the effort required to make a decision against the accuracy of the outcome. Also, the author explained, that the theory applied extensively to choice tasks. Related to this research, it is about factors that may influence errors and efforts required to make and influence decisions. Factors are characterized as related to task and/or context. Tasks in conjunction with choice is therefore characterized by the “response mode”, “task complexity (number of alternatives)”, “problem representation”, and “agenda effects”. Context variables investigate in “similarity of alternatives and the overall attractiveness of the alternatives”, “the variance in probabilities”, and “the presence or absence of alternatives that are worse than others on both error and effort” (Payne/Bettman/Johnson, 1988). Related to this research, there are several consequences for the design of an information security metrics aggregation method. Such a method should support different alternative tasks to enable making choices.

7.2.5.2 Information Overload, Aggregation, and Asymmetry

A major problem of decision theory is the available information on which the decisions are based. There are a lot of situations in which available information to support decision-makers are overwhelming. In this case, decision-makers have to choose the relevant information, locate and process them in the right manner to make a decision. Information overload is the phenomena if there is “more information available than necessary for processing a task and where this extraneous information has a detrimental effect on decision quality” (Speier-Pero, 2019). This leads to the use of heuristics for decision-making and reduces confidence in the decision.

To reduce information overload, the information is commonly aggregated. Information aggregation is defined as “the combining of information according to some type of integration rules” (Speier-Pero, 2019). These aggregations are mostly based on summarize operational activities in order to present them to decision-makers which do have an impact on decision-making quality. Speier-Pero (2019) showed, that more detailed information presented to decision-makers lead to more accurate decisions.

Reducing information necessary for a problem and adequate for decision-making leads to the use of dashboards in practice. (Yigitbasioglu/Velcu, 2012) conducted a literature review about different types of dashboards and recommended that they should be concise, simple, and intuitive to use. Decision-makers should be able to “zoom in” and “zoom out” in order to get more detailed information if necessary.

As described before, the responsibility for information security topics within organizations has shifted from technical employees to the management level. This causes, that there is also a knowledge-gap between these parties. The concept of information asymmetry deals with the imbalance of information between different group-members and is therefore related to behavioral decision making. Malekovic/Sutanto/Goutas (2016) showed, that the increase of information asymmetry leads to an increase of a group member’s manipulative tendency as well as the effectiveness of these manipulations. With an overall accepted information aggregation and the representation of these data, the manipulation tendency could be reduced.

7.3 Research Methodology

The design science methodology was used to develop a method to aggregate information security metrics into key information security indicators. This includes the method itself and the evaluation of this security metrics aggregation method based on previously defined requirements. This evaluation was conducted with the help of an instance of the method, a simulation, and an informed argument discussion. Section 7.3.1 describes the used design science approach in detail. To evaluate not just the requirements and the possible usability of the method, a second study was conducted to evaluate the understandability, clarity, and usefulness of the method as well as their instance. To evaluate these characteristics of a design science artifact, Sonnenberg/Vom Brocke (2012) suggested the use of expert interviews. Therefore, Section 7.3.2 describes the method used to conduct the expert interview series.

7.3.1 Design Science Methodology

“The result of design-science research in IS is, by definition, a purposeful IT artifact created to address an important organizational problem” (Hevner et al., 2004). An artifact can also be a decision support system, modeling tool, governance strategies, methods, and change interventions (Gregor/Hevner, 2013). Since the goal of this research is to develop a method, the article follows the design science approach proposed by Hevner et al. (2004).

Three design science contribution levels are described with examples of artifacts by the work of Gregor/Hevner (2013). Level 1 is a situated implementation of an artifact which is an instantiation of a software product or an implemented process. Level 2 describes a nascent design theory. Level 2 results are, for example, constructs, methods, models, design principles, or technological rules. Level 3 treats well-developed design theories. This article focuses on the development and description of a security metrics aggregation method (level 2 contribution) as well as an instantiation (level 1 contribution) to show the usability and usefulness of the proposed result.

Gregor/Hevner (2013) present not only the contribution levels but also a publication schema for design science research. This article follows the proposed publication schema to present the research. The design science process by Peffers et al. (2007) was used to generate the results. The first step within the process is the identification of the problem and the motivation of the topic, which is shown in the instruction, background, and related work of this article. The artifact description of this article includes the other steps of the design science process of Peffers et al. (2007). These steps consist of the definition of objectives, the description of the aggregation method, a demonstration of use in the form of instantiation and the evaluation of the result. The proposed publication schema by Gregor/Hevner (2013) ends with a discussion and a conclusion. The artifact description has to present and describe the artifact as well as the design search process and the evaluation "must be rigorously demonstrated via well-executed evaluation methods" (Hevner et al., 2004). The following design search process and evaluation methods were used:

- **Design search process.** The design search process was based on different requirements from the literature and practice. The literature review section shows that no current solution meets all the established requirements adequately. The combined current techniques to develop and visualize metrics as well as metric taxonomies lead to the development of the proposed method to aggregate metrics.

- **Evaluation.** An instantiation of the method is appropriate to show that the proposed method can be implemented in a working system (Hevner et al., 2004). Prat/Comyn-Wattiau/Akoka (2014) analyzed design science articles and concluded that the approach of instantiation with the demonstration of the use of the artifact is a valid evaluation method. Hevner et al. (2004) also present a set of five evaluation classes with 12 appropriate evaluation methods. This research is evaluated based on an experimental simulation of the instantiated method in comparison with existing measurement approaches of standards, which show the usability of the instantiation. Also, a descriptive informed argument based on the simulation was used to show that the established requirements are met.

7.3.2 Expert Interview Series

The expert interview series have multiple goals. The major goal is to evaluate the understandability, clarity, and usefulness of the information security metrics aggregation method as well as the results out of the method for information security managers. These characteristics are difficult to evaluate with just a simulation and an informed argument approach of the design science methodology. Using expert interviews was suggested by

Sonnenberg/Vom Brocke (2012) as an appropriate way to evaluate the understandability, clarity, and usefulness of methods.

There are various possibilities to conduct an expert interview series. The decision of choosing a semi-structured expert interview (Bortz/Döring, 1995) has the advantage of both worlds. Open interviews give the interviewees room for extended explanations where structured interviews ensure that all interviewees have the same questions. This ensures that the results are comparable but also allows the extraction of insights from the experts.

With these considerations, the following sections describe the different steps of the semi-structured expert interview series. Section 7.3.2.1 describes the goals of the interview series and their operationalization. The expert selection with the demographics of the experts is illustrated in Section 7.3.2.2. Section 7.3.2.3 explains the methodology to analyze the expert interview series.

7.3.2.1 Operationalization and Interview Procedure

The expert interview series has not just the goal to evaluate the understandability, clarity, and usefulness of the information security metrics aggregation method but also to gain insights from current practices in generating and developing information security metrics. Also, the possible advantage or disadvantage of using the proposed method and its instance in conjunction with the current approaches can be estimated by the experts. Besides the evaluation of the result, the interview series is also helpful to evaluate the used calibration of the simulation conducted within this research.

To give an orientation through the interview and make the analysis more comparable than an unstructured interview, an interview guide was developed in respect of the rules of good expert interviews by Bortz/Döring (1995). To support the described goals, the following areas with the included questions were discussed with the experts:

- **Current situation and simulation calibration.** To provide a pleasant interview situation, the interview starts with open questions about the current situation of information security metrics within the experts' organizations. Also, these questions were asked first, because no prior knowledge of this research is necessary. Therefore, to receive unbiased answers, the topic of the current situation was discussed first. To cover the topic, the experts were asked about the number of metrics they use to manage information security *(Q1.1)* as well as how they are developed *(Q1.2)*. A control question was used to evaluate if the developed metrics of the organizations are meaningful for the experts *(Q1.3)*. To evaluate the simulation performed within this research, a question was inserted before any explanation of the results. The most important and debatable variable within the simulation of the results was the number of vulnerabilities per system per month. Therefore, besides using available statistics out of the practice, the interviewees were asked about their opinion on how many vulnerabilities per system per month exist *(Q2.1)*.
- **Understandability, clarity and usefulness.** This part of the interview began with an explanation of the information security metrics aggregation method as well as the presentation of the instance with the goal to minimize vulnerable systems.

After this detailed information, the experts were asked, if the method itself, as well as the instance, is understandable *(Q3.1)*. This study does not use clarity explicitly because the construct understandability and clarity are considered as strongly related as Güver/Motschnig (2017) explained in their study. Also, the experts were asked if they would consider the method and the instance as useful and why *(Q3.2)*. After the whole interview, the experts were asked to quantify first the understandability of the presented results and second the usefulness of them from one (very understandable/useful) to five (not understandable/not useful).

- **Possible implications in practice.** Finally, to further get impressions about possible implications in practice, possible problems or other use cases, the experts were asked to give their overall impression about the method as well as the instantiation of it *(Q4.1)*.

7.3.2.2 Expert Selection

According to Bogner/Littig/Menz (2014), an expert is a person with a specific practical or experimental knowledge about a particular problem area or subject. Also, this person is able to structure this knowledge in a meaningful and action-guiding way for others. To cover the first part of this definition, the selected person has to have at least five years of experience in the area of information security within an organization. In this way, specific practical knowledge about the defined problem information security is ensured. The ability to structure the knowledge in a meaningful and action-guiding way for others is testified if the person is in a leading position within the organization.

The selection results in 16 experts who participated in the expert interview series between November 2019 and January 2020. The experts had at least five and at most 30 years of experience in information security. The average experience of all experts is 18.35 years. The experts are all in a leading position within their organizations. Thus, the participants are chief executive officers (1), chief information officers (1), chief information security officers (6), information security officers (4) and others (4). The four positions in the category “others” have different job titles but have the same tasks and responsibilities as (chief) information security officers. They are namely chief technical delivery managers, chief security architects or directors of security and resilience. All but two experts work in organizations that have more than 5000 employees and are globally acting. The average number of employees of all participated organizations was 101735. The required positions are normally available if the organization has one or more dedicated information security teams. These teams and the required leading positions for this expert interview series are often not available at small businesses. Therefore, the selected experts normally do not work in small- or medium-sized businesses.

7.3.2.3 Interview analysis

The basis to analyze the interviews is the qualitative content analysis according to the work of Mayring (2015). Mayring (2015) described three prerequisites to perform the qualitative content analysis. The definition of the material and how the material was created is described in the previous Section 7.3.2.1. The last prerequisite is the form in which the material is present. Normally, the analysis requires a textual basis (Mayring, 2015). Therefore, a full transcript of each interview was created and serves as the basis of all analysis steps.

After these definitions, an "analysis technique" has to be defined. There are various techniques available that are useful to analyze three different "basic forms". These forms are summarizing, explication and structuring. To answer the given questions and goals of this interview series, the analysis was done by the following steps suggested by Mayring (2015) for a summarizing analysis:

1. **Paraphrasing.** This step contains the deletion of text areas with no contribution to the goal and questions or which have little content. Also, a standardized level of language with a grammatical short form was created.
2. **Generalization.** This step takes the paraphrases and prepares them on an abstract level. Predicates are generalized in an equal form and theoretical assumptions are made in case of doubt.
3. **Reduction.** The reduction step generates the overall summary of opinions and answers to the questions. There, phrases with the same meaning are deleted, phrases of similar meanings are combined, very content-bearing phrases are selected and theoretical assumptions are made in case of doubt.

7.4 Security Metrics Aggregation Method

This section is structured according to the different steps of the design science research methodology process model of Peffers et al. (2007) with the extension of a second evaluation study. First, the objectives of the solution are given in Section 7.4.1 in the form of requirements. Second, the solution to meet the requirements is described in Section 7.4.2. This is followed in Section 7.4.3 by an instantiation of the solution in the context of minimizing vulnerable systems within organizations. Last, in Section 7.4.4, the evaluation according to the design science research approach is carried out by simulating outcomes of the instance and compare them to existing measurement approaches. To not just evaluate the requirements a second study evaluates the usefulness, clarity, and understandability of the proposed solution for information security managers in practice. This additional evaluation is present in Section 7.4.5 in the form of the results of the semi-structured expert interview series.

7.4.1 Artifact: Requirements

The method to aggregate security metrics should meet multiple requirements, which derive from past literature and the problems of practitioners described. The various metric taxonomies (Pendleton et al., 2017; Purboyo/Rahardjo/Kuspriyanto, 2011; Verendel, 2009) in the literature contain rules for good metrics which should be considered within an aggregation method. The main focus of the requirements are facing the problems which occur on the information security management and business management side described in Section 7.1 and 7.2. Ahmad/Sahib/Azuwa (2014) derive eight main criteria for effective security metrics, which also apply to aggregated metrics:

1. Meet security objectives
2. Quantifiable values
3. Simple measurement
4. Comparable result
5. Corrective action
6. Targeted audience/stakeholder
7. Security improvement
8. Align with business goals

These statements in conjunction with the needs for the management of Section 7.1 and 7.2 lead to the following five requirements and a more accurate description within the context of security metrics aggregation:

An instance of a security metrics aggregation method should...

1. *...be goal-oriented.* There is a need for security and business management to have an overview of the current status of information security based on abstract goals to be achieved. The goal orientation is needed because of the lack of technical knowledge of the management level. Security and business managers do not have the time to investigate deep into technical knowledge to understand each of the various technical metrics which are proposed by different standards and best practices. This is shown by the study of McKinsey & Company (Boehm et al., 2018) in which 1125 managers participated. Therefore, a security metric aggregation has to be goal-oriented to be useful for practitioners. The requirement summarizes statements 1, 6 and 7 of Ahmad/Sahib/Azuwa (2014).
2. *...provide quantifiable values.* All metrics and indicators should be "derived from precise and reliable numeric values" (Ahmad/Sahib/Azuwa, 2014). This means that not only technical metrics but all aggregations should meet this requirement. This requirement is also a prerequisite for the automation of the measurement process and data gathering. Statements 2 and 3 of the above enumeration are included in this requirement.
3. *...provide comparable results.* Results and metrics out of the aggregation method should be comparable among multiple organizations (Jafari et al., 2010) or different departments of an organization. This assumes that the data and metrics are not mutually exclusive or conflicting. This thus enables the necessary comparison of management reports and their containing information.
4. *...provide traceability.* If the values of metrics and reports fall below expectations, the management should have the possibility to trace back to find the root cause, especially if the result is an abstract indicator on a high management level. It has to be possible to trace the issue from the outcome backwards and from the

source forwards. The information asymmetry and overload are reduced but the disadvantages of them are mitigated because the initial data are available. This requirement is a basis and a prerequisite to meet requirement 5. The underlying statement of "security improvement" is included within this requirement and also contains the needs of the audience/stakeholders for an aggregation method.

5. *…allow the derivation of corrective actions.* The method should support a meaningful way to specify countermeasures and actions to improve the current status of the proposed metrics in a meaningful and traceable way. It should also help to guide and link different actions to business interests. The aggregated metrics should allow an improvement if adequate countermeasures are implemented. The prerequisite for the decision theory, namely, to have multiple actions to choose from, is supported by this requirement. The last statement, namely "corrective action", is covered by this requirement.

7.4.2 Artifact: Metrics Aggregation Methodology

The proposed method to aggregate security metrics is a three-step approach with a predefined set of available operations and rules. The result of the method leads to different standardized metrics that are linked in a tree structure over several levels. The aggregation is based on the set theory to guarantee comparable and traceable metrics. The following enumeration describes the security metrics aggregation method:

1. *Define a goal with a base set.* To meet the requirement that the result of the method should be goal-oriented, the first step is to define a concrete goal on the information security management level. It is important that this goal is defined on the most abstract level possible because it will be the key indicator with an assigned value at the end of the process. The management level can control the number of metrics on this level based on the number of goals which will be defined. For each goal, the whole method has to be carried out. This step goes further in defining a basic set of elements which are underlying to this goal. An example could be a goal like "minimize vulnerable systems" in which the basic set of elements are all technical systems of an organization. The base set can also be interpreted as the "scope" of the information security metrics aggregation. This leads to the possibility to adapted the base set to different stakeholders. In case of vulnerabilities, it is possible to set the scope to just the most critical production systems. This first step of defining goals with their base set is necessary to minimize the disadvantages of information overload.

2. *Define metrics to quantify the given goal.* This step can be done with the help of available methods like the GQM approach (Basili/Weiss, 1984) or other goal-based approaches. The second possibility is to use predefined metrics from available standards and best practices and a check whether they provide a certain aspect of the goal or not. This step also enables to take already available metrics out of the organizational infrastructure or develop them together with technical employees. It is not important which mathematical dimension, operation, or scale the metric shows, because each metric has to be linked to the base set from the previous step.

The rule to do that would be: "Statement of Metric" applies to "element of the base set". An example metric like "number of vulnerabilities" would be formulated as: "vulnerability" applies to "a system of the organization". In other words: "a system of the organization" has "vulnerabilities". Thus, each original metric is linked to the base set of the underlying goal whether it is a number, an average, or a division. The grounding of metrics to a base set allows information aggregation.

3. *Aggregate two or more metrics to indicators.* As all metrics are linked to the base set of step one, it is possible to aggregate two or more metrics to indicators with specific statements on higher levels. The operations are now derived from the set theory and consists of the operations: union, intersection, and set difference. The aggregation of "systems have vulnerabilities" intersects with "systems with old operating system" would be an indicator of "systems that have avoidable weaknesses". This step needs to be done iteratively until the goal indicator of step one is reached. The aggregation can be done based on subtopics of the base set, the questions of a pre-done GQM methodology or with the help of practical workshops by experts from the field. If base metrics cannot be aggregated and are not able to be integrate into the tree, it should be considered to exclude the metric. The exclusion of an indicator or metric shows that this metric might not be goal-oriented or useful in this context.

The result of the proposed method is a tree structure of different standardized metrics and indicators. Figure 7.1 introduces an overview of the method with the three steps described above. The whole tree can be used as a report-tool or dashboard. It is possible to quantify each node within the tree in the form of the number of elements in it. For example: "There are 5 systems with an old operating system in the organization". With the set theory in the background, it is also possible to generate comparable and illustrative percentages for each node in the tree. To achieve this, the percentage of elements in the node from the base set must be quantified. In the case of 100 systems (the number of elements in the base set), this leads to the statement: "5% of systems in the organization have an old operating system". Based on the audience/stakeholder, it is possible to report indicators or metrics from different levels of the tree. While the top management level just deals with the key indicators on the root element, technical employees could deal with the leaf elements. This leads to a structure that prevent negative effects of decision theories: (1) information aggregation (include all original information), (2) negative effects of information overload (show only necessary indicators), and (3) information asymmetry (detailed and transparent view).

7.4.3 Instantiation: Quantifying Technical Vulnerabilities

The usefulness of the security metrics aggregation method can be shown by using it to solve an instance of a problem (Peffers et al., 2007). A technical domain was chosen to show the effectiveness of combining technical metrics to a key indicator for the management of an organization. The domain is technical vulnerabilities within an organization, which is often reported as the number of vulnerabilities as the NIST 800-55 framework suggests (NIST, 2008). The following paragraphs include the three steps of the proposed method to identify technical metrics concerning technical vulnerabilities and aggregate them to a key vulnerability indicator.

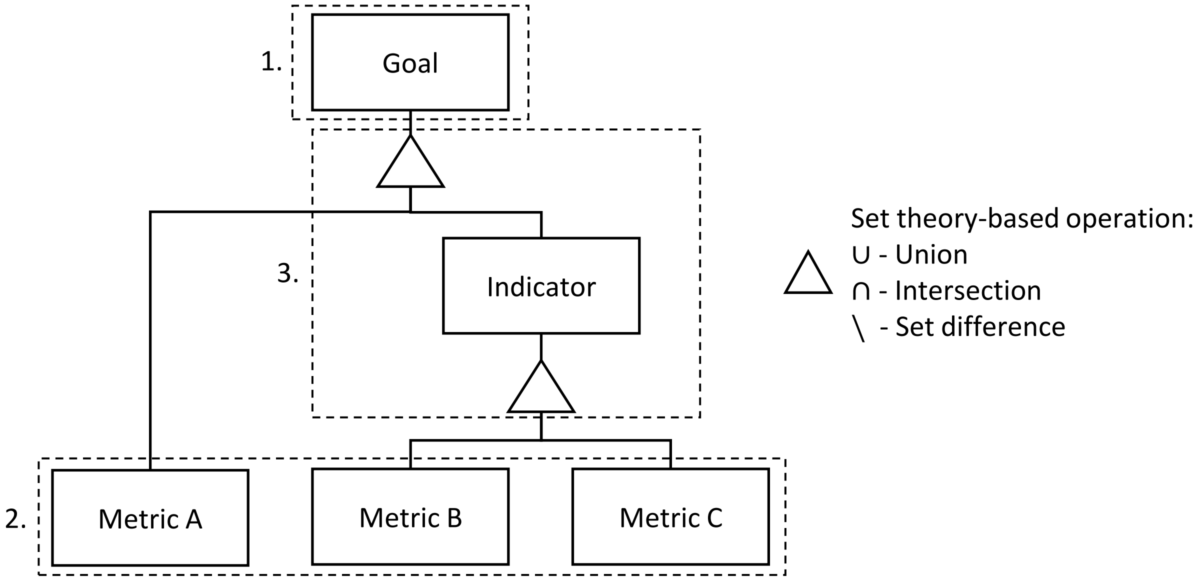

Figure 7.1: *Information security metrics aggregation method*

1. Define a goal with a base set. The goal of an organization is to minimize vulnerable systems within it and thus to minimize the attack surface of the organization. This leads also to the prevention of risks, because the risk just exists if there is an asset which has a vulnerability and a threat which can exploit this vulnerability (ISO/IEC, 2018). The base set or scope of this goal would be all technical systems within the organization. Systems encompass the personal computers of employees, servers, routers and other technical elements, which are connected to the network of the organization. As far as a technical system is reachable with an IP address, it is considered in the scope.

2. Define metrics to quantify the given goal. For a set of metrics illustrating the aggregation methodology, the GQM approach is used in combination with technical reports and studies of the industry to define suitable metrics for this instantiation. This step is shown in the following itemization as a result of the GQM methodology. Each metric has to be linked to the base set defined in step one. Thus, the link to the base set is also given on the metrics level below. The questions describe different aspects of the goal. If systems are not known, it cannot be tested and should be considered as vulnerable. Known weaknesses are described with question 2. Not patched and old systems are also describe vulnerable systems.

- Goal: Minimize vulnerable systems
  - Question 1: Are all systems in the knowledge base?
    - Metric 1.1: Number of managed systems. - Systems which are managed.
    - Metric 1.2: Number of all systems. - Base set.
  - Question 2: Which systems are weak?
    - Metric 2.1: Network vulnerabilities. - Systems with network vulnerabilities.

    - Metric 2.2: Application vulnerabilities. - Systems with application vulnerabilities.
  - Question 3: Are old systems in place?
    - Metric 3.1: Number of used blacklisted software. - Systems with blacklisted software.
    - Metric 3.2: Number of available software updates. - Systems with available software update.
    - Metric 3.3: Number of blacklisted software which can be replaced. - Systems with blacklisted software which can be replaced.

The suggested metrics are just examples of the quantification and one possible instance. Real reports do contain a lot more detailed metrics. The "2018 vulnerability statistics report" of edgescan (2018) defines 8 subcategories with 53 metrics just for application vulnerabilities. To keep the instantiation clear and understandable, the metrics themselves are on a more abstract level than in technical reports. However, the method allows the extension of this step and all steps with additional metrics.

3. Aggregate two or more metrics to indicators. The advantage of defining metrics with the GQM approach is that they are already clustered around topics and linked to certain aspects of the goal. This link is represented by the given questions of the methodology itself. This helps to aggregate the metrics from the bottom up but this is not necessarily required. Figure 7.2 shows the result of the aggregation process, which includes all possible operations, different metric levels and provides a single key metric for the information security manager, which represents the status of the organization regarding the defined goal. Vulnerable systems are the union of unmonitoring systems, which are considered to be vulnerable and known weak systems. Weak systems are a union of systems which can be updated and are therefore possibly weak and known vulnerable systems as a result of vulnerability scans. Updatable systems can be systems with available software updates as well as predefined blacklisted software, which can be replaced. Vulnerabilities can be derived from the network or applications. As mentioned in the previous step, the metrics are not complete and the instantiation shows an example of how to use the method.

The resulting metrics tree shows five different levels clustered in parts of important areas to quantify the vulnerability status of an organization. The different parts can be used to quantify different functions in the company. In this case, they could be the monitoring function, vulnerability management, and patch management. All the different functions are combined in one key vulnerability indicator for the top management. More detailed metrics for each function can be added if necessary.

7.4.4 Evaluation: Simulation and Requirements Validation

The simulation is based on the previously described result of the aggregation for system vulnerabilities. To illustrate the usefulness of the result and support the argumentation of the evaluation, a simulation based on artificial data was used. However, all data of the simulation are based on technical reports (Gartner Inc., 2017; Enterprise Management Associates, Inc, 2017)and are thus realistic. Additionally, the expert interview series was

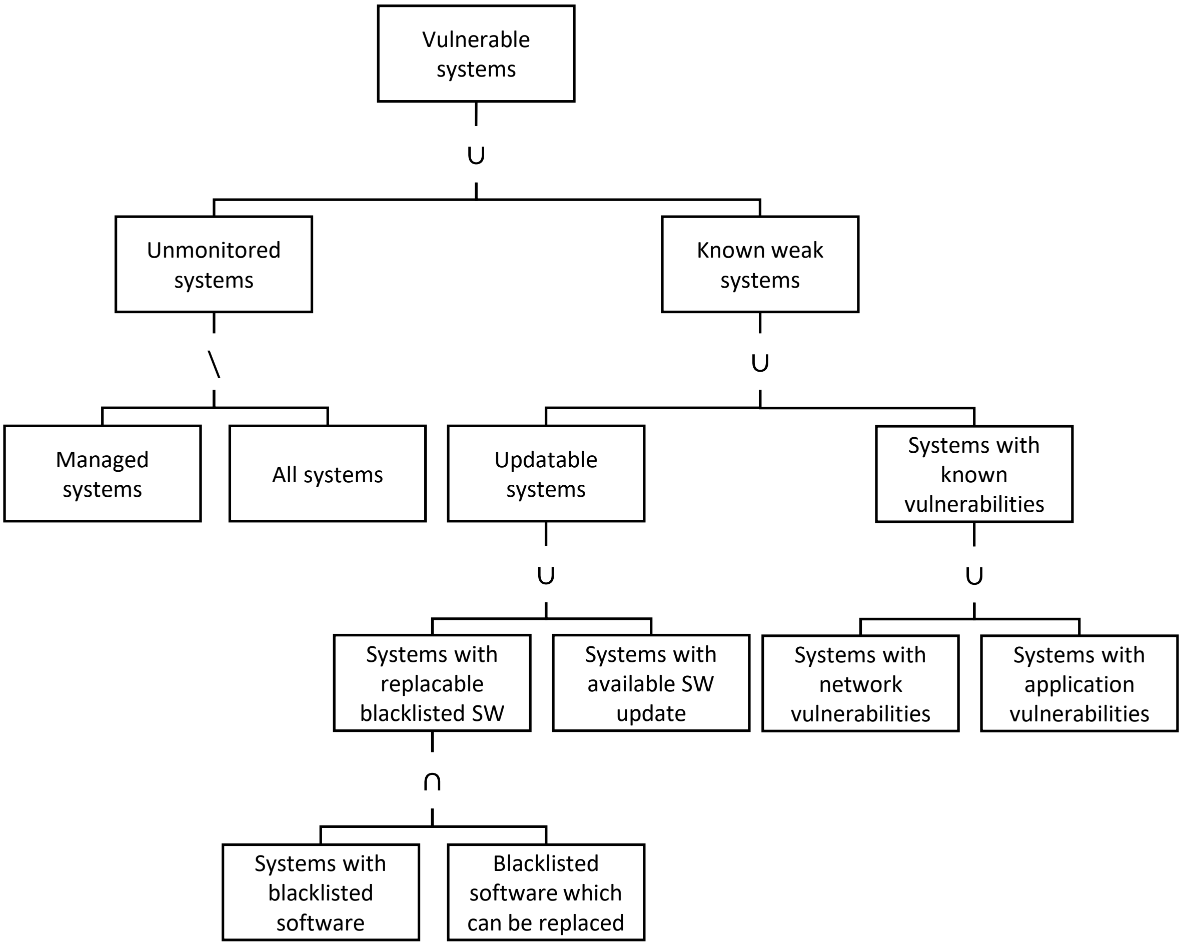
Vulnerable systems
∪
Unmonitored systems
Known weak systems
\
∪
Managed systems
All systems
Updatable systems
Systems with known vulnerabilities
∪
∪
Systems with replacable blacklisted SW
Systems with available SW update
Systems with network vulnerabilities
Systems with application vulnerabilities
∩
Systems with blacklisted software
Blacklisted software which can be replaced

Figure 7.2: *Quantifying the vulnerability status of an organization*

used to evaluate these data. The simulation of the result is further compared to the use of a common metric in the literature for illustrating the benefits of the presented method. In this case, the metric "Number of vulnerabilities" which comes from the NIST 800-55 NIST (2008) is chosen for this context. To compare the new metric of the proposed result for the management level with the common approach, the simulation just focuses on the key vulnerability indicator, the "Vulnerable systems". The characteristics described for the root metric should also be valid for the other metrics because all of them are based on the same base set and are created in a standardized way.

For simulating the metric outcomes, the Vensim PLE was used which is a fully functional system dynamics software from Ventana Systems Inc. This software is also used in research for different other purposes (Nazareth/Choi, 2015). The unit time frame of all simulations was set to a month and the model was run over 12 months. If the simulation were to take longer, the values would be significantly too high, because no countermeasures are simulated in the first instance to decrease the number of vulnerabilities. The model to simulate the commonly used metric "Number of vulnerabilities" is shown in Figure 7.3 where the "Vulnerable systems" simulation is shown in figure 7.4. Rectangles represent stocks which can accumulate or deplete over time. Double arrows are flows which are empty or infinite reservoirs which then affect stocks. All other variables are values which are either constants or are defined via a calculation for the given period.

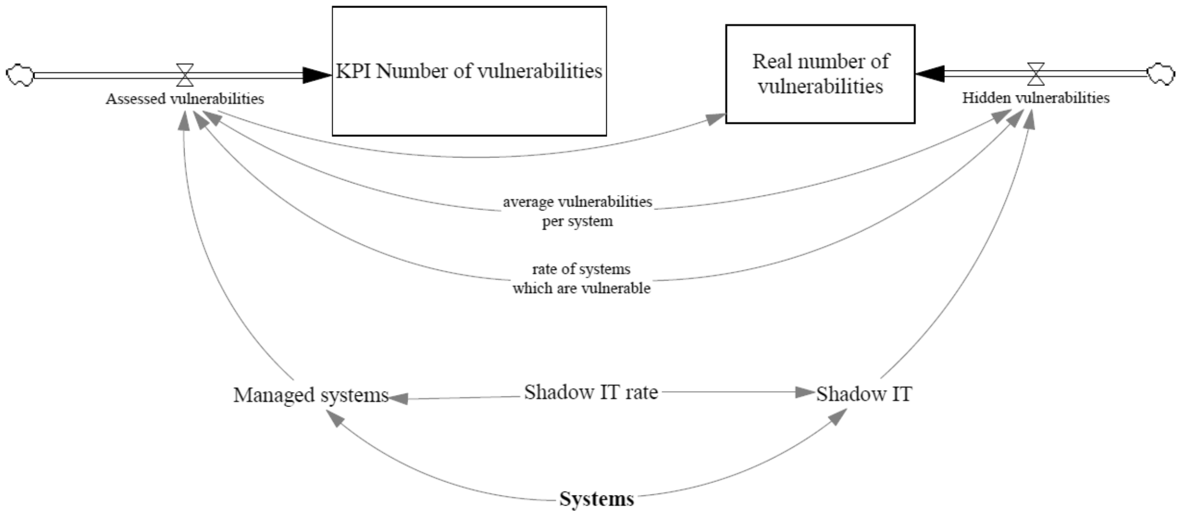
KPI Number of vulnerabilities
Real number of vulnerabilities
Assessed vulnerabilities
Hidden vulnerabilities
average vulnerabilities per system
rate of systems which are vulnerable
Managed systems
Shadow IT rate
Shadow IT
Systems

Figure 7.3: *Simulation of the metric “Number of vulnerabilities”*

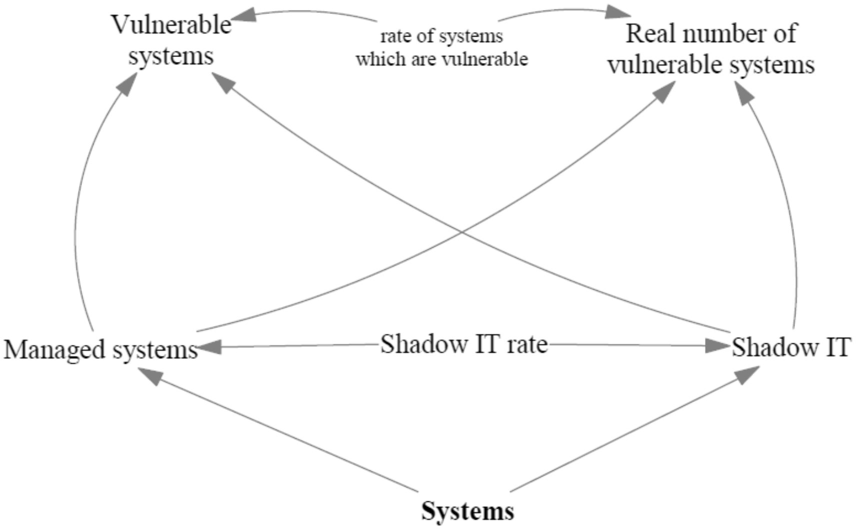
Vulnerable systems
rate of systems which are vulnerable
Real number of vulnerable systems
Managed systems
Shadow IT rate
Shadow IT
Systems

Figure 7.4: *Simulation of the metric “Vulnerable systems”*

All simulations are based on the following data:

- *Systems:* 100. This is set to a constant to illustrate the outcomes of the instance. The experts from the interview series complained that this would be a variable in practice but to illustrate the behavior of the system, a constant is appropriate.
- *Shadow IT rate:* 0.62 which is 62% based on the Gartner Inc. (2017) study which proposes that 38% of all IT spendings are controlled by the management.
- *rate of systems which are vulnerable:* 0.5. This value was also set to a constant to generate comparable results.
- *average vulnerabilities per system:* 10. This number is derived from a study of the Enterprise Management Associates, Inc (2017) which says that "Ten new vulnerabilities per system per month" exist in an organization. The variable itself is set to 10 vulnerabilities per system. The time frame of the simulation is set to one month which relates to 10 vulnerabilities per system per month within the flow "Assessed vulnerabilities". To further evaluate this variable, the experts were asked about their opinion of how many vulnerabilities per system per month exist *(Q2.1)*. The average opinion out of 16 experts was 19.25 vulnerabilities. Nevertheless, 10 vulnerabilities per system per month was mentioned by most of the experts (7) and is also the median of all answers. Therefore, the number was not adjusted after the expert interview series.

All simulated values are based on the assumption that no countermeasures are in place. So a stock variable like "KPI Number of vulnerabilities" does have a condition which adds vulnerabilities but their resolution is not modeled. This means that all new vulnerabilities are added to the existing one for each month. Also, both models contain not just the reported metric but also the "real number" of vulnerabilities or vulnerable systems based on the assumption that all information is known. This is mostly the "shadow it", which is not under the control of the management and thus cannot be security tested. The other assumption is that all vulnerabilities of the known systems can be found which is not common in reality. Thus, the common model of Figure 7.3 contains the real number of vulnerabilities from the "shadow it" and the other of Figure 7.4 contains the real number of vulnerable systems. Like the aggregation tree of Figure 7.2 shows, all systems which are not monitored are considered as vulnerable within this simulation.

Based on the simulation model and a comparison of the two outputs, the argumentation whether the requirements in Section 7.4.1 are met or not takes place. An exception is the last requirement, which does contain a modification of the simulation to include a possible countermeasure which represents a "corrective action". The following enumeration repeats the requirements for the aggregation method and discusses their fulfillment.

An instance of a security metrics aggregation method should...

1. *...be goal-oriented.* The resulted vulnerability metric aggregation is goal-oriented because of the method itself. The termination condition of aggregating lower-level

metrics is that the goal of the first method step is reached as a key indicator. If the termination condition is reached and metrics are not already included in the aggregation, they should be considered to be excluded. These metrics tend to be unrelated to the underlying goal or base set. The metric “Vulnerable systems” represents 12 other indicators which are useful for lower management or operational levels. This closes the gap between technical metrics and the management’s view. Also, a more detailed quantification of the goal is possible if more metrics are added to the aggregation methodology. For this example, the proposed metric “Number of vulnerabilities” also meets the requirement. The example shows their number which is a valid metric that represents the given goal. Other metrics considered by NIST 800, like “Percentage of vulnerabilities mitigated” (NIST, 2008) are not goal-oriented because the metric itself quantifies the process of mitigating vulnerabilities which do not represent the actual state of vulnerabilities within the organization. The method would exclude this metric because it cannot be linked to the base set “systems”. If just this metric were to be reported, there would have to be a lot more metrics like the total amount of found vulnerabilities, the amount of still open vulnerabilities or others to interpret the value in a meaningful way.

2. *...provide quantifiable values.* The set theory approach allows the assignment of a number to each type of metric. Even for binary questions, the method allows the assignment of an overall value for a basic set which would be the number of elements within the node of the tree structure. An example could be a checklist with the question if an employee has participated in security training. In this case, the base set is all employees and the metric is the number of employees who participated in security training or the percentage of all employees who participated. The values have to be precise and reliable (Ahmad/Sahib/Azuwa, 2014). This requirement can be tested with the help of the simulation.

   Figures 7.5 and 7.6 show a comparison between the reported values of the metrics versus the real number which are present within the organization. The metric “Number of vulnerabilities” in Figure 7.5 shows that there are significantly fewer vulnerabilities reported than there are existing within the organization. The reason is that shadow IT cannot be tested and is not considered to be vulnerable. The report is optimistic and includes the vulnerabilities which are found in the organization. The metric “Vulnerable systems” in Figure 7.6 on the other hand is much higher than the real number of vulnerable systems. The reason is the assumption that unmonitored systems are likely to be vulnerable. This result is explained by the pessimistic approach saying that all unmonitored systems are vulnerable.

   The total difference between the real and the reported values is significantly less on the proposed metrics aggregation approach and therefore more precise and reliable. This shows that the presented methodology makes it possible to produce pessimistic security assessments within organizations.

3. *...provide comparable results.* The comparison of different metrics is important in practice to benchmark own values against others. It helps to identify best practices or better approaches and discuss possible improvements. There are two different relevant cases. The first is a comparison of different departments or locations of an organization. Most of the time, a chief information security officer receives reports from different information security officers and has to combine, consolidate and

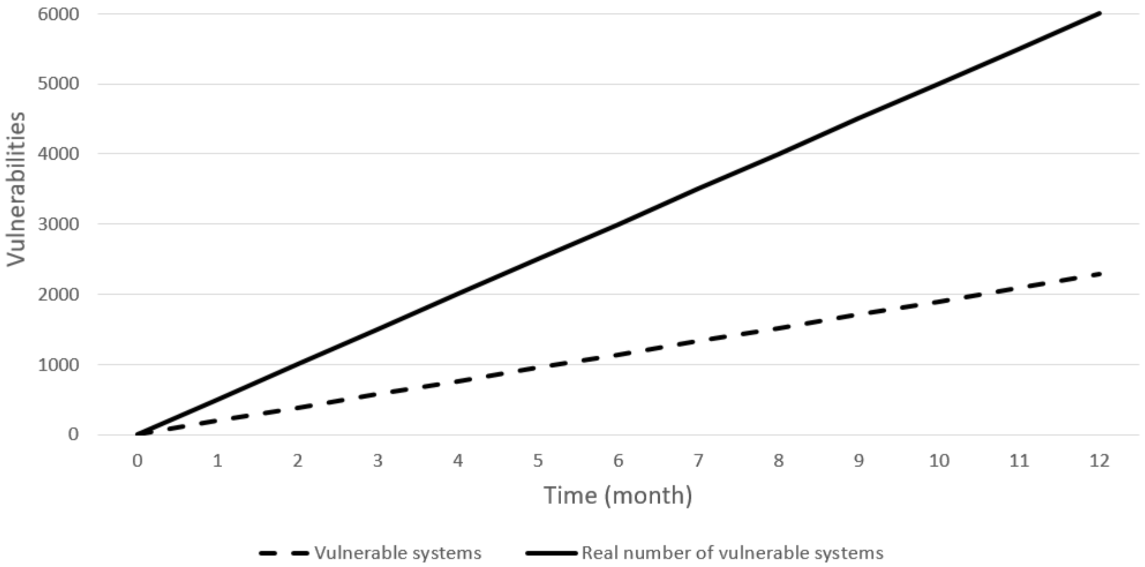

Figure 7.5: *Assessed vs. real number of vulnerabilities*

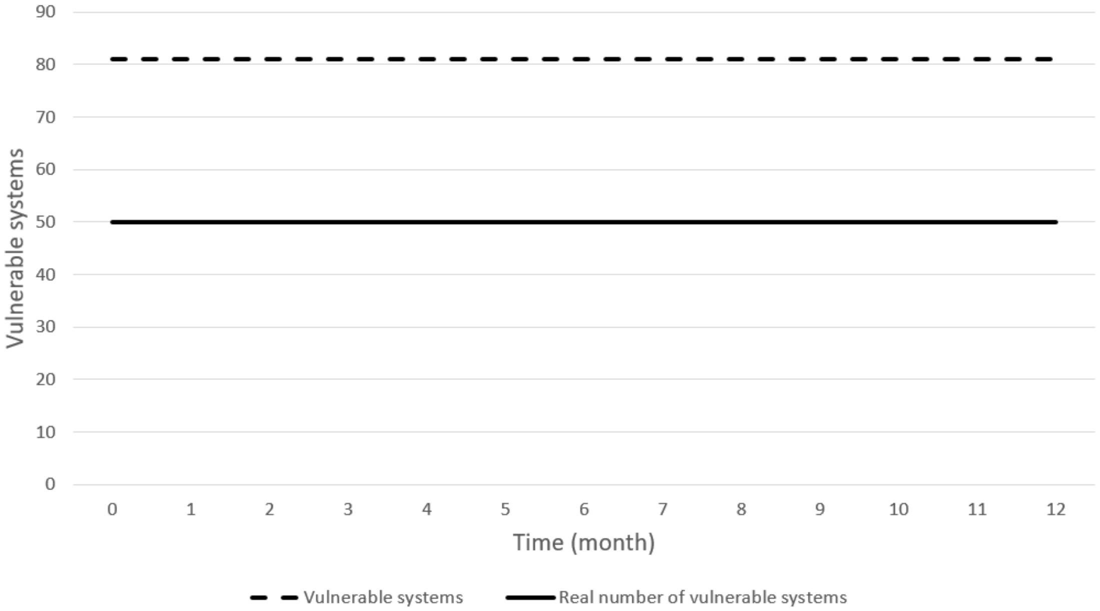

Figure 7.6: *Assessed vs. real vulnerable systems*

compare them. The second case is a comparison between different organizations. This comparison is often the basis for an exchange of experiences with specific techniques to improve the information security level.

A problem with the common approach is that the base set of elements on which the data is collected is not part of the metrics. For example, it is possible that different departments of an organization use the same systems and each of them collects their vulnerabilities. On the management level, these vulnerabilities would be added to an overall metric which then includes the same vulnerability multiple times. The definition of the basic set and the usage of the set theory does mitigate this problem. It is more transparent regarding which elements and underlying data the metrics were collected and is thus more comparable.

A general problem with comparing absolute numbers is that there is no defined reference. If one organization reports 10 vulnerabilities and the other 100, it is not clear from which organization the other can learn. This situation often relies on the underlying base set. If the first organization has 2 systems and the second has 10000 systems, it could be argued that the second organization performs better and can advise the first one. If both have the same number of systems, it could be the other way around. All the problems with current metrics described are not present for the metrics proposed in this research. The solution is the possibility of two representations of each node within the aggregation tree. The first one is the absolute number of elements within the node, which is important for all employee levels and the management to estimate the workload. The other one is the percentage representation based on the basic set. The simulation result shown in Figure 7.6 would be 82% of vulnerable systems and also 82 vulnerable systems because the basic set is 100 in this case. If there is a second organization with the same values but 200 systems, a report would consist of 41% percent of vulnerable systems but also a total of 82 vulnerable systems.

4. *…provide traceability.* The management should be able to understand the reported metrics without detailed technical knowledge and, if necessary, trace back to look at how the metrics are achieved. It is important for the management not just to understand the different components and aspects of the metric but also to find the root causes if a metric should be under the expectations. The illustrated aggregation method with the instantiation shows that the requirement is met by structuring the metrics as a tree. Also, an explanation of different metrics is possible without detailed technical knowledge or background. The metric "Number of vulnerabilities" does not allow an explanation of any aspects within it. Questions on what are vulnerabilities or which systems are included are not answered by reporting this metric. A technical employee has to explain a lot to illustrate which aspects are part of the metric, how the collection was carried out and which systems are affected. The information security management also has to explain the business management in the hope that they understand it (Boehm et al., 2018). This is mitigated by the metrics tree by supporting the different parts of the key indicator and allowing the management to trace back to leaf nodes of the tree.

5. *…allow the derivation of corrective actions.* The most important requirement is the possibility to derive corrective actions and countermeasures from the metrics and indicators. The "Number of vulnerabilities" only allows one action from the definition of the metric: reduce vulnerabilities. This action is the goal at the same time, but the question remains: which actions are appropriate to reduce the vulnerabilities in an efficient and effective way or even which part of the underlying problem should be dealt with first. Often, a cheap countermeasure can have a big impact and thus is prioritized higher by the management than others which are on the one hand very useful but expensive. Also, it is not possible to trace downwards to find appropriate weaknesses on a more detailed level and derive actions from the "Number of vulnerabilities". With the resulted aggregation of metrics, multiple actions can be defined. A few examples would be to replace blacklisted software, update old software or just include unmonitored and not security-tested systems in the monitoring. These are just a few examples of countermeasures to reduce vulnerable systems that can directly be derived from the aggregation tree.

The requirement also includes the aspect that countermeasures have to allow an improvement of the metric or indicator. For this purpose, the simulation was slightly modified by adding a countermeasure which reduces the shadow IT within the simulated organization. Figures 7.7 and 7.8 show the adjusted model which slightly reduces the shadow IT by 5 percentage points per month.

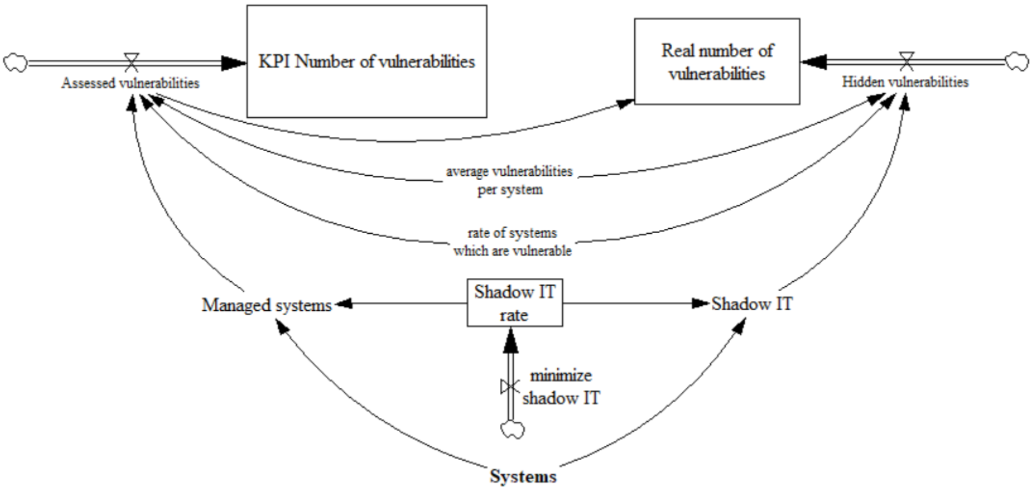
KPI Number of vulnerabilities
Real number of vulnerabilities
Assessed vulnerabilities
Hidden vulnerabilities
average vulnerabilities per system
rate of systems which are vulnerable
Managed systems
Shadow IT rate
Shadow IT
minimize shadow IT
Systems

Figure 7.7: *Simulation model of vulnerable systems with countermeasure*

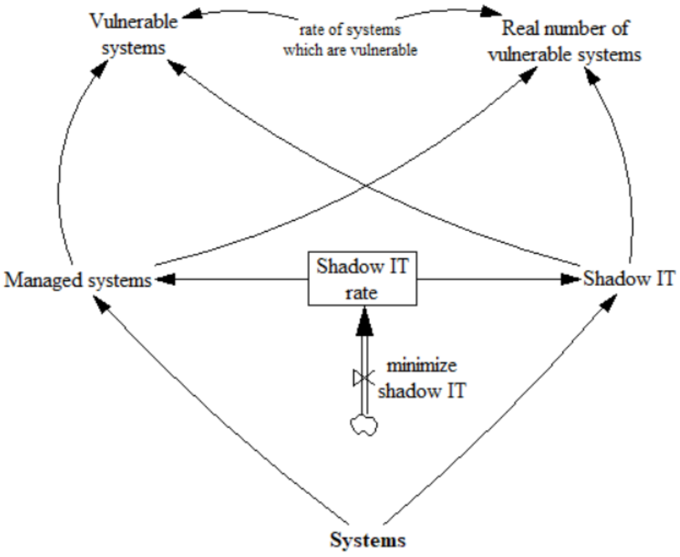

Figure 7.8: *Simulation model of number of systems with countermeasure*

Figure 7.9 shows the result of the "Vulnerable systems" indicator by applying the countermeasure in comparison with the metric if no countermeasure was applied. Because of the supported pessimistic assumption that all unmonitored systems are vulnerable, the metric decreases the number of vulnerable systems and the situation improves according to the given goal. Figure 7.10 shows the same situation with the common approach to count the number of vulnerabilities but it can be seen that the vulnerabilities increase over time and the situation deteriorates. The explanation of this phenomenon is that the reported value approaches the real amount of vulnerabilities. By applying the monitoring to new systems, more vulnerabilities can be found. The problem comes into effect if employees have to explain the increasing amount of vulnerabilities to the management level, while their job to achieve the goal is to reduce them. This can lead to not taking different useful countermeasures to avoid a need for explaining them to the management. In contrast (see Figure 7.9), the monitoring of new systems also include these systems that are not vulnerable and the metric “Vulnerable systems” approaches the real number of vulnerable systems. It can be seen that the proposed aggregation supports the given requirement of the possibility to derive corrective actions. Moreover, the proposed metrics tree include possible countermeasures (action alternatives) for the management.

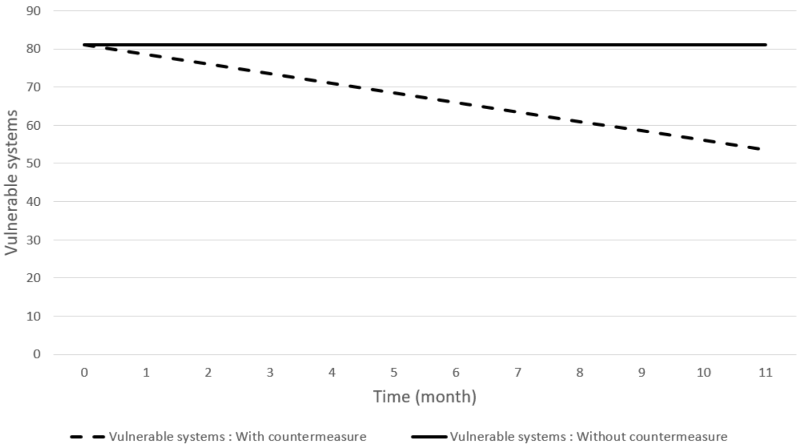

Figure 7.9: *Vulnerable systems with reducing shadow IT*

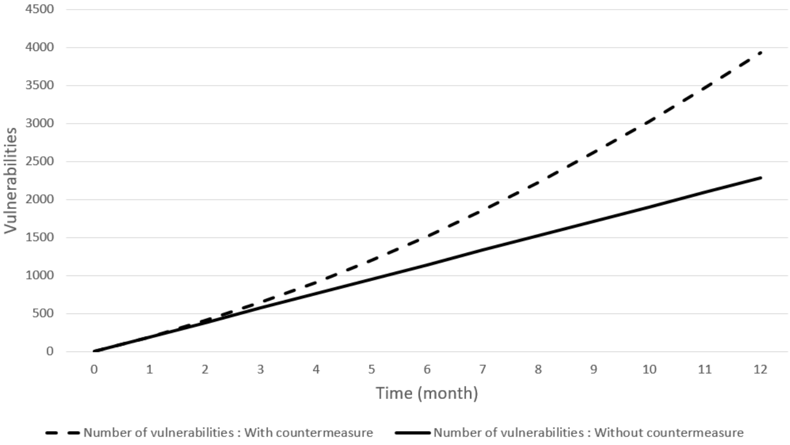

Figure 7.10: *Number of vulnerabilities with reducing shadow IT*

7.4.5 Evaluation: Expert Interview Results

To evaluate the proposed results of this research, 16 information security experts of organizations were asked about their opinions based on three goals (Section 7.3.2.1). This section is structured according to these goals. The current situation of information security metrics development in practice is shown in Section 7.4.5.1. Section 7.4.5.2 describes the possible advantages and also the concerns of the experts in using the method and the developed instance in practice. The last Section 7.4.5.3 points out possible implications and possibilities for extensions that were derived out of the expert interviews. Also, an example of how to extend the instance to meet further requirements of experts is shown. All goals were analyzed based on the whole interviews and the method outlined in Section 7.3.2.3. The main questions which ensure the extraction of the knowledge are outlined in each section.

7.4.5.1 Current Information Security Metrics Development

The first goal was to show how information security metrics are used and developed in practice and to ensure that the proposed method can significantly improve this situation. To reach this goal, the questions on how many information security metrics are used by the experts *(Q1.1)* and how they have been developed *(Q1.2)* were asked. The control question was to ask if the experts consider these metrics to be meaningful *(Q1.3)*.

The number of used information security metrics differs greatly:

- **0-1.** Five experts do not use metrics to control the information security status of their organizations. These organizations either started to implement metrics and planning them or make decisions pure based on controls from best practices and standards like ISO/IEC 27000. The reports of the experts are done ad-hoc to answer questions from the upper management.
- **10-50.** Four experts have a reduced amount of indicators. These indicators are mostly calculated numbers which are based on multiple other metrics.
- **200 and more.** The other experts have a large amount of information security metrics that are not aggregated in any form.

Three different approaches to define these metrics were identified out of the interviews.

1. **Self-definition.** The first approach is to self-define the information security metrics. These experts use internal workshops or self-developed methods to produce their metrics. The explained methods and characteristics of the metrics are based on available approaches like the CVSS score or risk management processes and then adapted to their needs. The resulting information security metrics of these experts are also considered useful by them. A few concerns arrived when it comes to compare them with other departments and organizations.
2. **Standards and best practices.** Most experts use metrics out of standards and best practices. The ISO/IEC 27000 series, NIST 800 series, Trusted Information Security Assessment Exchange (TISAX) and others are used to either take the defined metrics directly out of them or to use the included controls and define at least one metric for each of these controls. This leads to a large number of information security metrics. All experts who follow this approach mentioned that not all of them are useful for them. They are not useful to take actions out of them, are not meaningful or not measurable at all. Therefore, some of the experts in this category filter the metrics within these standards based on workshops and choose these which are meaningful and measurable for them.

3. **Data driven.** One expert explained that the metrics derived out of available data within their systems. To generate these metrics, they assessed the available data and looked for interesting and useful characteristics that would be helpful to quantify the current information security status. There, the cost-benefit ratio has to be in mind to consider these metrics as useful. A small organization would have a huge overhead and not much of a benefit of implementing such a solution.

4. **Requested.** The last approach is to define the metrics based on the requests of different stakeholders. This was the upper management and regulatory requirements. These metrics were considered mostly as not useful by the experts.

The current situation to use and develop information security metrics in order to quantify aspects of the information security status of organizations confirms the discussed problems out of section 7.1 and 7.2.

7.4.5.2 Expert Opinion about the Results

The main purpose of conducting a semi-structured expert interview was to evaluate the understandability, clarity, and usefulness of the information security metrics aggregation method and the developed instance. The characteristics of understandability and clarity are seen as equal within the interviews (see section 7.3.2.1). The whole interview transcripts were used to analyze possible advantages and concerns the interviewees see in using the results of this research. The questions on what the experts think about the understandability of the method and the instance *(Q3.1)* and if the experts consider the method and the instance useful and why *(Q3.2)* are included in the interview guide.

At the end of the whole interview, the experts were asked to rate the understandability and the usefulness from one (very understandable/useful) to five (not understandable/not useful). All answers are between one and two while the average understandability was 1.125 and the average usefulness was 1.375. This shows, that the proposed results are considered as very understandable and very useful for information security managers in practice.

Five main advantages of using the method and the instance in order to quantify vulnerabilities are described by the interview partners:

1. **Reporting to the top management.** The method allows developing a low number of KPIs which are useful to report to the top management of an organization. The reduced number of KPIs is useful to easily get an overview of the information security status of the organization. The proposed method allows the management and control of the situation and is therefore very useful.

2. **Extendability.** The experts saw different opportunities to extend the solution based on their needs. The sub-trees of the instance can be extended down to a more technical level and the method could be used for other information security areas like awareness. A very interesting insight is, that such a tree is very useful to start with a monitoring solution. Sub-trees can be implemented step by step and can be

extended from time to time to other parts of the tree. The beginning to implement such solutions was a major concern within organizations.

3. **Explanation of information security metrics.** The methodology itself allows a structured and analytical way to deal with the complex problem of information security metrics development. Most of the experts have the problem that the discussions about which metrics are useful, which are measurable or definitions terms can be very emotional. These discussions prevent them from even starting to monitor the information security status. An understandable and acceptable methodology makes the beginning a lot easier in practice. Tho proposed result out of the methodology shows a tree structure of different metrics. This tree structure explains the metrics itself. It shows their calculation and how they have to be tested and monitored as well as the underlined base set. This explanation allows further to give the tree different departments or even external partners which can collect the described data in order to report them back. The proposed visualization is well based, sound and makes the metrics more understandable despite their derivation and abstraction. The last consideration of the experts within the explainability was the advantages of the instances to support managers of small and medium-sized businesses. They are often information technology managers with operational tasks. Also, they are responsible for the information security within the organization but do not have the knowledge and know-how to deal with this complex area. Besides the available standards and best practices, the proposed solution can help these managers to get an overall understanding of the different areas which are important to deal with information security based on the trees.

4. **Derive actions.** The experts considered the tree structure as a kind of a decision-tree. A manager can use different sub-trees to derive prioritized actions from the management perspective. Different information security areas can be traced back and root causes of problems can be found. This is able not just for the information security management but also on an operational level. The tree illustrates multiple possibilities to improve the overall KPI on top of the tree which allows deriving more actions than before. Not just actions to improve the situations are visualized but also possible deficits can be pointed out. For example, the instance to quantify vulnerable systems indicates whether an organization has a Configuration Management Database (CMDB), whether all systems are tested or which assets are monitored.

5. **Comparable results.** The experts noticed that the aggregation is based on a common denominator which allows comparing the metrics. The results out of the information security metrics aggregation method could also allow a combination of different metrics out of other methods and compare different organizations. The aspect of comparability is very important for the information security management. The experts mentioned a further concern which makes comparability even more important. With this instance, it is avoided that “everyone calculates the numbers as they want and that they are manipulated for their benefits”.

There are not just positive effects and advantages mentioned by the experts. Very few possible concerns were raised, which is why these are already shown here in a single mention. The following concerns were present in the expert interviews:

1. **Unclear definitions.** There are concerns about the different terms used within the instance. If a manager just sees the tree and the term "'Vulnerable system" the question of what is a system arises. Therefore, for each term, an exact definition has to be provided. This avoids emotional discussions within organizations.

2. **Finding the right metrics.** The method itself do not help in finding the right metrics.

3. **Data collection.** Four experts had concerns about the possibility to collect the required data to quantify the metrics for the whole instance presented. In contrast, four other experts said that they could collect all the required data straight out of standard software in place. The experts were very divided on this topic.

4. **Prioritization, weight, and criticality.** The most concerns arise that the instance does not support the prioritization of actions, weight to different security areas, the criticality of systems or the criticality of vulnerabilities. The prioritization of actions and the weight of different sub-trees is not provided by the instance as well as the methodology itself. This has to be done by information security managers with respect to the organization's needs, boundaries, and compliance policies. For information security managers, a general overview of all systems with all the vulnerabilities is useful. To report to the top management, these numbers are not meaningful because they can not assess the impact or criticality of these numbers. If there are 10 vulnerable systems, the top management would ask if this is good or bad, if the services can still operate or what have to be done. Also, the KPI does not produce enough pressure to the top management if the vulnerable systems increase to 11 in this example but the affected system is highly critical. The need for fast actions is not included. Therefore, the information security managers asked for possibilities to support the criticality. The proposed method gives solutions for this but an example was not included. The first possibility is to reduce the scope of the whole instance to "critical systemsïn order to report to the top management. The second possibility is to extend the instance with filter-metrics. Figure 7.11 shows an example with the goal to report the "systems with critical vulnerabilities" and the "critical systems with critical vulnerabilities". The KPI "Vulnerable systems" is the head KPI of the proposed instance of Section 7.4.3, the grey filled rectangles are the reporting goal while the grey bordered rectangles are the used filters combined with an intersection.

7.4.5.3 Possible Implications and Impressions of Experts

Finally, the experts were asked about their overall impressions of the information security metrics aggregation method as well as the proposed instance *(Q4.1)*. The impressions were very positive which leads to multiple suggested further use cases and possibilities of usage based on the experts' backgrounds. The experts considered four different areas of using the proposed method which also could be interesting areas of future research:

1. **Extension to support the financial view.** It could be possible and is requested by the information security managers to use the method to support and include

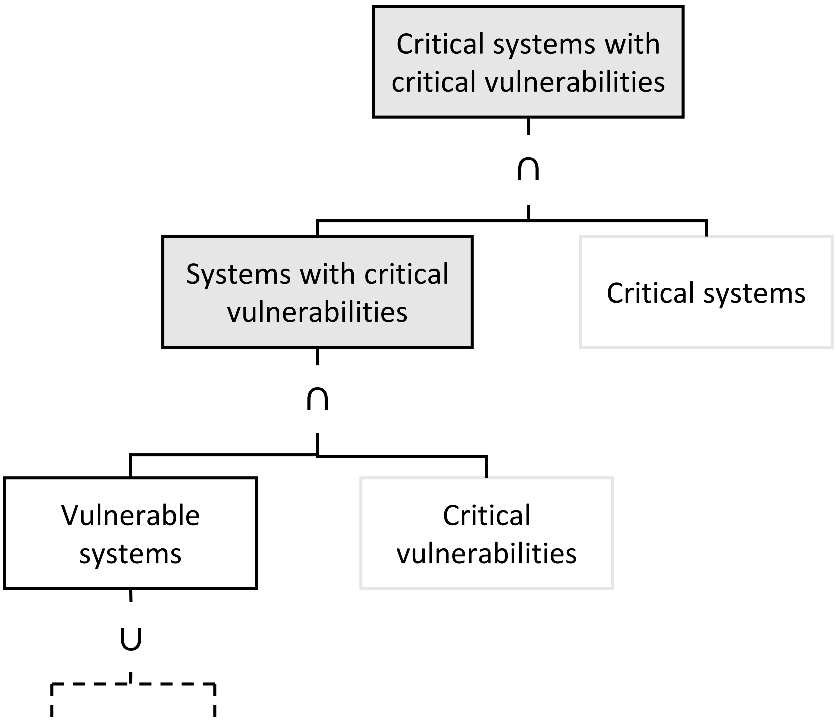
Critical systems with critical vulnerabilities
∩
Systems with critical vulnerabilities
Critical systems
∩
Vulnerable systems
Critical vulnerabilities
∪

Figure 7.11: *Example to support reporting goals*

the financial view to the different metrics. This means, that each metric could associate with risks and the possible financial implication for the organization. This would enable not just to support the information security management but also the financial or even the board management. Further, the connection of the different metrics to the individual business goals would be useful for information security managers as well as business managers to better illustrate the value of information security within organizations.

2. **Further areas.** The experts suggest the usage of the method for each information security area which includes access control, threats, awareness, risks, operational security, and compliance. Some possibilities would be the usage for other areas for example within the product-environment to quantify security and safety aspects of products.

3. **Development of a common standard.** It was suggested by the experts to use the method to generate metrics and their aggregation for each part of information security within organizations. These instances could be tested by a variate of organizations to create a commonly accepted information security metrics standard. Such a standard with a mapping to existing standards and best practices would show the rightmetrics which are commonly used in practice. The current trend in practice is the use of rating systems in the information security area. Such a standard could provide such a rating in order to provide a comparison of different service providers and therefore is usable for decisions on outsourcing.

4. **Information security management dashboard.** A great opportunity to work with the method would be a system that implements the suggested solution. This solution should have the necessary interfaces to collect all data automatically out

of the organization, aggregate the metrics and present them as a dashboard. All metrics which are not able to collect automatically could be forced to manually insert by the responsible managers. It could also be a possible opportunity for defining a decision support system.

7.5 Discussion and Directions for Future Research

This research study contributes to the question of how information security metrics can be consolidated and prepared for the information security management of an organization. Therefore, the research proposes a standardized method to aggregate metrics in the information security area based on requirements, which are asked by practitioners and researchers. The information security metrics aggregation method consists of three steps to achieve a goal-oriented, quantifiable, comparable and traceable aggregation which also allows the definition of appropriate actions to improve them. An example instantiation to quantify the goal of minimizing vulnerable systems within organizations shows the usefulness and effectiveness of the proposed method. The evaluation consists of an argumentation of each requirement with the help of a simulation. Additionally, a semi-structured expert interview was conducted to evaluate the possible understandability, clarity, and usefulness of the result for information security managers in practice.

There are goal-oriented approaches that help managers to develop metrics and there is also a lot of work with predefined metrics in place. A standardized way to aggregate them from bottom to top is to have a key indicator for the defined goal that was not in place before. As shown in this research article, the method can be combined with the existing goal-based and standard approaches of security metrics development and extends them to generate a suitable security metrics framework for multiple levels of an organization. By using the method, the stated problems from the literature and practice with the lack of structure, clarity, and comparability in information security reports could be mitigated, and the gap between technical employees and the business management reduced. Also, different problems in decision theory like the effects of information overload, information asymmetry and information aggregation on management-decisions can be reduced by using the method. The proposed results contribute to the literature by allowing to extend current information security management standards with the possibility of aggregating the supposed security metrics to their security concepts. Also, different standard security dashboards and reports can be developed based on the aggregation method.

The way to aggregate security metrics given provides a pessimistic measurement of the security status which compensates for the fact that not all information is given at any time. An example provided is that not all systems of an organization might be under security monitoring. An optimistic measure like the number of vulnerabilities would just count the known number which does not include vulnerabilities from systems that are not security monitored. The proposed method supports a pessimistic measure by providing the possibility to count the systems as vulnerable and count them equivalent to systems with known vulnerabilities. A countermeasure that includes such unmonitored systems in the security monitoring system, as a result, improves the security status. An optimistic measure would worsen the metric because more vulnerabilities would be found. This could lead to the assumption that the information security department of an organization does not increase but rather decreases the security level of the organization. The proposed method supports pessimistic measurement and thus reacts positively with appropriate countermeasures.

According to information overload theory, the reduction of information leads to the lower effectiveness of decisions. The proposed solution shows that the aggregation can be done by a base set aggregation without losing the information based on an index. This process allows dashboards with the opportunity to "zoom in" and "zoom out" which was asked in literature and by practitioners. All information is available for the higher management level which leads to more accurate decisions because the uncertainty is reduced. Also, managers may feel more comfortable in their decisions. Furthermore, the method allows a standardized reporting from technical employees to the information security management without the support of the tendency to manipulate data from bottom to top as a result of information asymmetry between the group members. Despite current theory, the aggregation of data may not lead to the loss of information and therefore to the described disadvantages of these theories.

As the semi-structured expert interview reveals, the current information security manager does not use a standardized method to aggregate or even develop information security metrics. There are standards and best practices in place but they do not provide a suitable method to develop key security indicators. This leads to problems for small- and medium-sized business managers who have to deal with information security management but do not have enough expertise. The proposed method and the resulted instance can lead to an explanation of the most important areas of information security and how to measure them. Besides the explanation of the information security landscape itself. The interviewees expose several other advantages like the explanation of the metrics and their calculation, the possibility to use the metric for reporting even to the top management, the extendability and usefulness to use the method for other areas, the possibility to derive multiple countermeasures and the production of comparable results. The last advantage was also a disadvantage using the instanciation.

The experts also explained possibilities for further usage of the method which leads also to future possible research. The method could not just be used to quantify vulnerabilities but also for other goals. The security area consists of multiple topics like awareness, infrastructure weaknesses, access control or operational issues like patch management or incident management. All areas have a goal from the management perspective which could be quantifiable by instantiating the method. By using this method, a possible information security dashboard could be developed which could be implemented in multiple organizations for a discussion base to collaborate and improve the security knowledge and status of a whole region. Even small- and medium-sized businesses with relatively few resources could participate and use the method or the results of this method to understand the nature of information security better, try to first collect the relevant data needed to quantify the metrics, and begin to improve their security status. A possible way to do this would be to define an information security metrics standard and link it to existing ones.

The most asked solution for the interviewees is a system solution with the needed interfaces which collect all the necessary data to quantify and calculate the metrics automatically and show them as a management dashboard. To develop such a technical system, the proposed method could be used to quantify all relevant information security management goals and evaluate these instances. This would lead to the concept of a comprehensive information security management dashboard. This concept would serve as a template and specification for researching and implementing an automated system which would be the beginning of a possible decision support system for information security managers.

If using the proposed solution, the management of an organization has to be aware of the nature of information security metrics. The instances are just able to show known information and in the presented instance the known vulnerable systems. A typical problem in measuring information security vulnerabilities is the existence of so-called zero-day vulnerabilities and exploits. By using the method and an instance of it, the management has to be aware of possible unknown vulnerabilities that are not covered by the measurement. Also, the use of metrics does not prevent the organization from being attacked. Nevertheless, practitioners have to measure the current state of the information security as well as to know if there are known vulnerabilities in place. Without these measures, it is not possible to get resources for the necessary actions, closing the vulnerabilities or even start trying to monitor the organization's infrastructure. The research shows the usefulness of measuring known vulnerabilities and weaknesses to manage information security, show different areas of interest, serve possible actions, and compare different organizations. A study of Flexera (2018) also shows, that just 14 out of 19,954 vulnerabilities were zero-day vulnerabilities. Experts of the interview series confirmed, that they never saw a breach out of a zero-day exploit in practice because it is not necessary to find or use one. There are many open known vulnerabilities with available exploits available, which can be easily used by attackers without the time-consuming task of finding a new vulnerability. By using metrics to assess the known vulnerabilities and reduce them, the risk of being successfully attacked can be mitigated. The proposed solution would help to achieve this.

Each research shows limitations and also future research out of these limitations. In this case, the research shows one instantiation of the information security metrics aggregation method through the goal of minimizing vulnerable systems within an organization. To further illustrate the usability and effectiveness of the method, other phenomena like awareness, infrastructure weaknesses or access control should be instantiated and evaluated. The effectiveness of the resulted instance was shown with the help of the simulation method and artificial data. The simulation itself illustrate the behavior of the metrics in a specific scenario but not in reality. Nevertheless, behavioral data from a semi-structured expert interview series shows that the supposed method, as well as the instance, is understandable, clear, easy to use, and useful. An implementation in practice with a case study to evaluate the method is missing and should be considered for future research. Such studies are a possibility to not only evaluate the method and the instances themselves but also to find new relations between the collected data and understand the different areas which would be quantified better. An adaption of the method to use it for other disciplines cannot be excluded and could open up interesting solutions and new research areas. An example could be the application of the method to develop solutions for another context like cloud computing and cloud service providers. In this case, information security is an important topic to illustrate customer trust but difficult to quantify (Lang/Wiesche/Krcmar, 2018). The aggregation method could help to reduce the complexity of certain information security metrics in the cloud context on a customer level as an information security indicator.

7.6 Conclusion

Reporting information security issues for the management level of an organization is still a challenging task in terms of structure, clarity, and comparability. Also, current research asks for closing the gap between technical security metrics and the management view on security issues. Therefore, this research uses a design-science methodology to develop an information security metrics aggregation method based on requirements to overcome the stated problems in practice. The method should be goal-oriented, quantifiable, comparable, traceable and the management would have to derive appropriate actions from the metrics.

This article shows that the problems can be mitigated by aggregating technical information security metrics in a standardized way, based on the set theory. This results in a tree-structured aggregation of different technical metrics to key indicators which represents a security management goal. An instantiation on the example of vulnerabilities and the simulation of the outcomes shows the usability and effectiveness of the proposed method. A semi-structured expert interview shows the understandability, clarity, and usefulness of the method and the instance from the perspective of information security managers.

The method can be used by security and business managers to develop a standardized security metrics framework and a reporting tool at the same time. Also, appropriate countermeasures to improve the current state of the security status can be derived from the results and thus make better decisions. Also, the result enables a cross-organizational comparison of information security metrics. Researchers could use the method for the development of decision-support models, security metrics framework development, security status quantification or the observation of the effects of certain countermeasures within organizations. The use of the method for other metrics besides the security area could be a possible research field.

8 A Conceptual Information Security Assessment Dashboard for Organizations

Title	A Conceptual Information Security Assessment Dashboard for Organizations
Authors	Diesch, Rainer[1,2] (rainer.diesch@tum.de) Krcmar, Helmut[2] (helmut.krcmar@tum.de) [1]fortiss GmbH, Guerickestraße 25, 80805 Munich, Germany [2]Technical University of Munich (TUM), Boltzmannstraße 3, 85748 Garching, Germany
Type	Journal
Outlet	Journal of Management Information Systems
Publisher	Elsevier Inc.[3]
Ranking	VHB-JOURQUAL 3[4]: A
Status	Submitted
How to Cite	-
Individual Contribution	Conceptualization, Methodology, Investigation, Data Curation, Writing - Original Draft, Writing - Review & Editing, Visualization

Table 8.1: *Bibliographic details for P5*

[3] https://www.elsevier.com/

[4] https://vhbonline.org/vhb4you/vhb-jourqual/vhb-jourqual-3

A Conceptual Information Security Assessment Dashboard for Organizations

Abstract: Information security assessment is a major task for information security managers and remains a challenge in practice. There are various standards and best practices that suggest metrics. However, there is a major challenge: these metrics are usually not clear, understandable, actionable, and useful for information security managers of organizations. Therefore, this study investigates the development of a standardized dashboard to assess the information security status of an organization. An information security metrics aggregation method based on the design science methodology was used to generate 10 key indicators for information security managers. To evaluate the results, a focus group - also called workshop - was conducted with experts from a leading global organization. The study enables security managers to assess the information security status of an organization in a standardized way. The dashboard allows information security managers of all hierarchies to derive corrective actions, compare metrics, and overcome common issues related to information overload, asymmetry, and aggregation.

8.1 Introduction

Information security remains a major challenge and task for organizations (Soomro/Shah/Ahmed, 2016). Business models and services are based or even fully dependent on data (Knapp et al., 2006). Especially digital transformation efforts leading to more digital services and business processes which increase the dependence on data steadily. The importance of information security is also shown in a study by Altimeter, a Prophet Company. They asked 554 participants about their top priorities for technology investments in 2019. After investing in “cloud” (37%), 35% prioritize “cybersecurity” in conjunction with digital transformation (Solis, 2018). Information security has to be considered not just to further develop businesses but also to secure them. In 2018, the average cost of a data breach was \$3.86 million (Ponemon Institute LLC, 2018). When there is a data breach, organizations incur not just financial losses but also legal and reputation repercussions are a risk for organizations (Tu/Yuan, 2014). A study by Grant et al. (2014) also shows that security, along with reputation and dependency on data, was one of the most prominent risks faced by businesses in the high to very high risk rating. Therefore, practitioners and researchers focus more and more on information security.

Information security is a top priority for the board and top management, as well as technical employees of an organization. Therefore, standards and best practices such as the ISO/IEC 27000 series (ISO/IEC, 2018), or COBIT (ISACA, 2012), deal with information security management and governance aspects. Other standards such as the NIST SP800 series (NIST, 2018b), or the Standard of Good Practices from the ISF (ISF, 2018), deal more with technical aspects to protect information. The present focus in information security is due to the responsibility shift of the issue of information security from technical employees to the management level of organizations (Yeh/Chang, 2007; Ashenden, 2008; Ransbotham/Mitra, 2009). This goes further to the extent that managers today are fully responsible for security problems (Abu-Musa, 2010; Soomro/Shah/Ahmed, 2016).

Despite these standards and best practices, data breaches and information security issues are present in the daily news. An organization has to know at any given point in time, how secure their information systems are (Mermigas/Patsakis/Pirounias, 2013). A major challenge is finding an effective way for technical employees to communicate information security assessments to supervising managers. An appropriate method to assess and report the information security status of an organization is by using metrics. Different metrics are described within standards and best practices. The ISO/IEC 27004 (ISO/IEC, 2009) or NIST SP800-55r1 (NIST, 2008) deal with information security metrics but, by their own account, don't cover the minimum information security requirements (NIST, 2008). These metrics often measure the effective implementation of countermeasures, not if the countermeasures are effective (Bayuk, 2013). Furthermore, a survey of McKinsey & Company (Boehm et al., 2018) identified the lack of clarity, structure, and consistent data within information security reports. Multiple authors in past literature also mentioned these shortcomings and see the need for a holistic view on information security (Savola, 2013; Soomro/Shah/Ahmed, 2016), the gap in research to measure information security in a standardized or automated way (Alshaikh et al., 2014; Arabsorkhi/Ghaffari, 2018; Diesch/Pfaff/Krcmar, 2018; M'manga et al., 2019), and the need for information security dashboards (Dogaheh, 2010; Maier et al., 2017; Al-Darwish/Choe, 2019; Tewamba et al., 2019; Diesch/Pfaff/Krcmar, 2020) as a basis for information security decision support need to be addressed. Therefore, this study develops and evaluates a conceptual information security assessment dashboard from the information security management perspective of an organization.

The remainder of this article is structured as follows. Section 8.2 shows existing work on information security management practice, information security metrics, and dashboards as well as theoretical background and the basis literature used to develop the results. The used methodology to develop the information security dashboard is illustrated in Section 8.3 followed by the evaluated information security dashboard from the management perspective in Section 8.4. Section 8.5 provides a critical discussion of the results alongside possible future research directions. The article closes with a conclusion in Section 8.6.

8.2 Background and related work

Information security assessment is part of the information security management of organizations. Therefore, the first part of this section introduces information security management in theory and practice (Section 8.2.1). Measurement with metrics is the main and most widely used method for assessing information security. Therefore, the second part (Section 8.2.2) deal with current literature on information security metrics. Theory and practice refer to the use of dashboards in conjunction with information security, which leads to Section 8.2.3. Finally, the possibility of contributing to essential theory is set out in Section 8.2.4. Here, an introduction to decision theory and the essential aspects of this article like information overload, information asymmetry, and information aggregation is given.

8.2.1 Information security management

Information security refers to the aim of ensuring business continuity and minimize business damage (von Solms/van Niekerk, 2013). The term “Information security” in a business context is defined by the protection of all information that can be transmitted with or without technical systems Diesch/Pfaff/Krcmar (2018). This means that not technical systems but also the awareness of employees is included within this definition. An Information Security Management System (ISMS) is used to achieve information security within organizations and protect business objectives. An ISMS is defined as a “part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security” (ISO/IEC, 2005).

Organizations rely on standards and best practices to implement information security management. The most commonly used framework is the ISO/IEC 27000 series (ISO/IEC, 2018). These standards play an important role in organizations (Siponen/Willison, 2009). Other standards such as the NIST 800 series (NIST, 2018b) or ISF (ISF, 2018) are more technical but are often used in conjunction with higher-level governance standards. An important aspect of information security management is the monitoring part. This task is the basis for reviewing, maintaining, and improving the information security status of an organization continuously, which is required to certify against the given standards. Certificates are not only useful for the organizations’ self-control but primarily a reputation mechanism and therefore have an impact on business outcomes. The standards recommend multiple metrics to monitor the information security status, but these metrics do not cover the minimum information security requirements (NIST, 2008), do not sufficiently address the overall security position (Jafari et al., 2010), do not take the realities of daily work into account Hedström et al. (2011), and are not comparable among different organizations (Jafari et al., 2010). Several authors also mentioned other shortcomings of the standards and best practices in place. Standards are very generic in scope and tend to be abstract (Siponen/Willison, 2009), they consist of too much information (Mijnhardt/Baars/Spruit, 2016), rigorous empirical studies are missing (Siponen/Willison, 2009; Diesch/Pfaff/Krcmar, 2018), and regional differences which are “individually useful [...] but do not provide a cohesive and explicit framework to manage information security” (Smith et al., 2010). Also, suggested policies within the standards rarely cover the necessary information security issues (Doherty/Anastasakis/Fulford, 2009). In general, the implementation of an information security standard does not necessarily mean that security is adequately provided (Yeniman Yildirim et al., 2011; Lee/Geng/Raghunathan, 2016). “The only way of answering critical questions, for information security is to test the security of the information entities” (Yeniman Yildirim et al., 2011).

To overcome some shortcomings, Diesch/Pfaff/Krcmar (2020) suggest a comprehensive model of information security factors for decision-makers with 12 management success factors to help information security managers as well as business managers to get an overview of this complex topic. These authors interviewed 19 experts and concluded the need for a dashboard and reporting standard for key security indicators which is currently not available in literature. They also suggest the use of these metrics as goals for the information security management of an organization (Diesch/Pfaff/Krcmar, 2020).

8.2.2 Information security metrics

Information security metrics are well discussed in the literature. Several authors use different definitions for metrics, indicators, measurement, measure, countermeasure, and assessment. For example, Azuwa/Sahib/Shamsuddin (2017) presented six different definitions of metrics. For this research, the following definitions are used:

- "A **metric** assigns data onto some kind of scale in order to correctly represent some security attribute of a system under consideration" (Verendel, 2009).
- The **measurement** is "the process of estimating attributes of an object" (Pendleton et al., 2017).
- **Measure** and **countermeasure** are considered the same as safeguards by Jafari et al. (2010). Therefore, they mean to "improve the overall information security state by selecting the best security countermeasures to protect their information assets" (Yulianto/Lim/Soewito, 2016).
- An **indicator** is often used as a synonym for "metric". This article uses **indicator** as the "combination of the data provided by the metrics, so that they provides useful information to the organization" (Herrera, 2005).
- A security **assessment** is "a commonly used practice that estimates the present cyber security posture of an information system" (Qassim et al., 2019) or in this case, an organization.

Diesch/Pfaff/Krcmar (2018) conducted a systematic literature review on security metrics and developed a research agenda. They found that measurement is needed to capture the current information security status, manage, and make well-informed decisions. Current literature focuses on individual metrics but does not cover an overall view from the management perspective. This link is important because existing metrics are not always understandable for information security and business managers (May, 1997). Another problem is that current metrics are linked to the individual security programs and are therefore not comparable with other departments or organizations (Geer/Hoo/Jaquith, 2003; Jafari et al., 2010). The first step to overcome this limitation taken by Diesch/Krcmar (2020). They assigned the individual existing metrics in the literature to existing management goals and suggested the use of this assignment in order to develop a dashboard with key security indicators for the management of organizations. Other authors also mentioned the lack of proper resources and assessment tools which are necessary for maintaining information security (Qassim et al., 2019). Practitioners also recommended automating the security assessment (M'manga et al., 2019) which is just possible, if there are standardized metric approaches available.

8.2.3 Information security dashboards

Haqaf/Koyuncu (2018) studied the key skills of information security managers. Out of 16 key skills, four are about understanding different security parts like the security architecture, network security, or the information security issues from a management point-of-view. Assessment of different aspects is present three times. Identify best practices for risk management is one of them. In summary, eight out of 16 key skills are about understanding, assessing, and identifying different information security aspects. Bojanc/ Jerman-Blažič (2008) showed the usual risk management steps for information security management. Assessment of aspects like business assets, treats, and vulnerabilities is present in each of the six steps mentioned. The sixth step itself consists of "monitoring". The challenge is not just to implement security policies once but to monitor and adjust them as well as countermeasures over time with respect to the current situation, which is not present in most academic literature (Samonas/Dhillon/Almusharraf, 2020). Also, prior research falls short in identifying and integrating characteristics of business, threats, and countermeasures important for understanding information security value (Kumar/ Park/Subramaniam, 2008).

Therefore, information security managers, as well as business managers, rely on dashboards and frequently generated reports to respond quickly to changing conditions. Dashboards serve as decision support tools for information security and business managers (Yigitbasioglu/Velcu, 2012). However, research on information security dashboards is rare. Authors deal with visualization aspects of dashboards or individual metrics (Savola/ Heinonen, 2011; McKenna et al., 2016; Maier et al., 2017). Yigitbasioglu/Velcu (2012) conducted a comprehensive multidisciplinary literature review to reveal critical issues faced by organizations while implementing a dashboard. The recommendations within this review also focus on visualization aspects that are dependent on different aspects such as the purpose of the dashboard, tasks, user groups, and features. They also asked for research to select the right metrics and indicators because the dashboard's success could very well depend on them. Bayuk/Mostashari (2013) also said that "there are no standards for what types of metrics should be included in these dashboards". A standard information security dashboard with standardized metrics would be useful for prospective tasks such as assessment automation, cross-organizational comparison, or decision support systems, which are requested by researchers and practitioners.

8.2.4 Decision theory

Decision theory is "a powerful tool for providing advice on which management alternative is optimal given the available information" (Polasky et al., 2011). Decision theory is a part of basic management science, because managers have to make decisions most likely under uncertainty. There are related theories and concepts out of this definition that deal with the different alternatives or with the knowledge available. Because there is a high probability that information is either under asymmetry or aggregated, managers need to choose heuristics. A major finding of the behavioral decision theory is, that heuristics can perform similar to optimal decision rules (Csaszar/Eggers, 2013).

Several aspects of decision theory come into place when using metrics and dashboards for decision support purposes. Information overload is a situation where there is more information than is required. The theory points out that "extraneous information has a detrimental effect on decision quality" (Speier-Pero, 2019). Information overload leads to the use of heuristics. On the other hand, information aggregation is used to overcome information overload and combine available information. Key indicators within dashboards are usually aggregated metrics. By comparison, aggregation itself can reduce decision quality (Speier-Pero, 2019). Dashboards itself have the advantage to reduce information asymmetry. Information asymmetry is the imbalance of available information between different members of a group and can cause the manipulative tendency of these group members for their purpose (Malekovic/Sutanto/Goutas, 2016).

8.3 Research design

The design of an artifact is by definition a result of design science research in information systems (Hevner et al., 2004). (Gregor/Hevner, 2013) said that an artifact is not only a purposeful IT artifact but can also be a decision support system, a modeling tool, a governance strategy, a method, and a change intervention. The expected result of a dashboard is also considered as an artifact. Therefore, this research is developed based on the design science research guidelines by Hevner et al. (2004). To develop the dedicated artifact, a design science process is used that complies with the guidelines. A process that respects the guidelines were introduced by Peffers et al. (2007). It consists of *(1)* a problem definition, *(2)* a definition of the objective, *(3)* the design and development, *(4)* a demonstration and evaluation, and *(5)* the communication of the results. The following enumeration describes each step in detail:

1. *The problem definition* is set out in Section 8.1 and Section 8.2. In addition, current problems are discussed in the context of the results of this article (see Section 8.4).

2. *The definition of the objective* is based on the problems described in the literature and practice. A dashboard of information security metrics from the management perspective should consist of a limited number of important key information security metrics that cover the information security status of an organization and are easy to understand. The metrics should be tractable, actionable, and comparable. Therefore, the artifact would consist of different key indicators and a detailed description of their calculation.

3. *Design and development.* The results are based on previous work which consists of information security management success factors (see Section 8.2.1) and technical information security metrics of the literature (see Section 8.2.2). The design of the dashboard is based on the aggregation of these technical information security metrics to key indicators with the help of the existing information security metrics aggregation method. This methodology is based on three steps. First, the goals for the information security management must be defined with a base set of elements. Second, the metrics must be defined and linked to these base sets. Third, the metrics must be aggregated based on the operators union, intersection, and set difference.

4. *The demonstration and evaluation* of the artifact was carried out with the help of the developed metric trees (see Section 8.4.3). Use-cases and examples were developed to demonstrate their conceptual use in practice. Following the examples of previous research, this research uses a focus group - also called workshop - with practitioners in attendance to evaluate the developed conceptual dashboard. A focus group methodology in general “is a way of collecting qualitative data, which - essentially - involves engaging a small number of people in an informal group discussion (or discussions) ‘focused’ around a particular topic or set of issues” (Wilkinson, 2004). Because other authors such as Tang et al. (2010) or Peffers et al. (2007) called

this methodology "workshop", this article also uses the term. Peffers et al. (2007) used workshops in "Case 4: Developing a Method at Digia to Generate Ideas for New Applications That Customers Value" to validate the new method. Also, other researchers such as Tang et al. (2010) used a workshop to validate their research with industrial participants. The workshop within this research was conducted with "Munich Reinsurance Company (Munich Re)", a leading global reinsurance company located in Germany. The workshop was attended by three (senior) underwriter of the cooperate underwriting team, one cyber-risk specialist which deal with the business and law perspective, and two members of the internal risk management team. These six participants are according to the recommended number of participants for a focus group between six and twelve (Onwuegbuzie et al., 2009). These participants cover a wide range of perspectives: the experience of multiple risk assessments of customers, the business perspective, and the internal information security perspective. The workshop aimed to introduce previous work, discuss the developed results with a critical view on the detailed metrics and the implications of these results. A protocol was prepared and subsequently agreed with the organization for completeness and accuracy. Also, one participant sent written feedback with notes within the metric trees. Based on the feedback, two improvements were made within the trees.

8.4 A conceptual dashboard of key security indicators

This section is structured according to the three steps of the information security metrics aggregation method. Thus, Section 8.4.1 presents the information security management goals and the definition of the base set elements for them. Section 8.4.2 includes the metrics definition and the linkage to the base set. Section 8.4.3 presents the information security assessment dashboard with all aggregation trees for each information security management goal. Insights from experts with the evaluation and recommendations of the workshops are present in Section 8.4.4.

8.4.1 Information security management goals and key indicators

The basis of the conceptual information security management dashboard is the goals of information security managers. These goals are required to further define and aggregate information security metrics. Section 8.2.1 introduced information security factors from the management perspective in current literature. These 12 factors are "physical security", "vulnerability", "infrastructure", "awareness", "access control", "risk", "resources", "organizational factors", "CIA", "continuity", "security management", and "compliance & policy". All of these factors have an impact on the information security management decisions and therefore, serve as factors that can be optimized from the management perspective. The first step of the security metrics aggregation method used (see Section 8.3) involves assessing a base set to each information security management goal. Table 8.2 shows the different information security management success factors, their transformation into goals and the assignment of a specific base set.

Factor (Diesch/Pfaff/ Krcmar, 2020)	**Goal**	**Base set**
Vulnerability	Minimize vulnerabilities	Systems
Resources	Optimize resources	Tasks
Awareness	Maximize awareness	People
Access Control	Maximize restrictions to resources	System identities
Physical Security	Maximize physical access restrictions	High critical physical devices
Infrastructure	Maximize hardening level and communication security	Infrastructure components
Risk	Mitigate risks based on acceptance level	Assets
Continuity	Maximize the ability to deliver intended outcome	High critical systems
Security Management	-	-
Organizational factors	-	-
CIA Triad	Ensure CIA	Assets
Compliance & Policy	Maximize rule conformation	Rules

Table 8.2: *Information security management goals and their base sets*

Organizational factors cannot be optimized. These are the size, sector, or other specific organizational factors that are not within the decision-making context of an information security manager. Also, security management is described as an operational process to derive policies, countermeasures, and all other related processes within the framework of information security standards and best practices. As discussed in Section 8.2, the implementation and improvement of processes do not necessarily mean that the information security status is improved. Also, processes vary between different organizations. Therefore, this research does not focus on information security operations metrics. All other factors are assigned a goal and a base set. The following itemization describes the definitions of the different base sets:

- **Systems:** Systems are all devices and endpoints that “speak” IP. Thus, every endpoint that provides an IP address is considered a system in the scope of the goal to minimize vulnerabilities.
- **Tasks:** All tasks that need resources like budget, technical resources, or people.
- **People:** Each person within the company or which holds valuable information is considered in scope for this goal.
- **System identities:** All user and password combinations stored within systems. It is important to not only count the real persons within an organization but all identities available.
- **High critical physical devices:** Unlike **Systems**, these are physical devices that could provide multiple IP addresses. Physical security can be characterized more precisely based on physical devices.

- **Infrastructure components:** These are all physical and virtual components within the infrastructure. Examples are routers, firewalls, servers, and personal computers that are connected to the infrastructure of the organization.

- **High critical systems:** Based on feedback from practitioners, the scope for the goal to maximize continuity is restricted to a subset of **Systems** that are highly critical for the organization. The effort to ensure continuity is very high, which is the reason for this restriction.

- **Processes:** This base set describes the set of processes such as risk management, problem management, incident management, or others. All operational information security-related processes and project states are within the scope of the base set.

- **Assets:** All organizational assets are in scope to ensure "CIA" or mitigate the risk level. An asset can be a system, a person, or a system identity to mention just a few. The other goals with their subsets serve as input for this goal, which comes from the definition of risks. "Risk occurs when assets are vulnerable to threats" (Yeh/Chang, 2007).

- **Rules:** Rules are not just policies from the individual organization but also legal aspects of which an organization must comply.

8.4.2 Metrics to quantify aspects of the goals

Each information security goal serves as key indicators for the information security management of an organization. To quantify these factors, information security metrics must be defined, linked to the information security management goals, and assign the metrics the base set. The basis for defining the metrics for each information security management goal was a state-of-the-art literature analysis in conjunction with the goal-question-metric approach. These information was used for defining information security metrics and linking them to the information security management success factors (see Section 8.2.2). This work was used as a basis for the second step of the security metrics aggregation method and assigned each metric the corresponding base set. Appendix C includes one table for each information security management goal with the corresponding question and metric out of previous work Diesch/Krcmar (2020) as well as the extension of this research. The extensions include additional metrics that were not present in the existing literature, the assignment of the base set, and the selection in order to quantify the given information security management goal. The column "Notes" includes different decision reasons, for example, the reason why a metric has been excluded, newly included, or modified within this step.

The result contains 83 different information security metrics that are linked to the base set of the information security management goals. These can be used in the next step to aggregate them to key indicators for the information security management dashboard.

8.4.3 A conceptual information security dashboard

The last step of the information security metrics aggregation method generates the resulting information security dashboard. Each information security goal is quantified with a key indicator. These are:

- Vulnerable systems
- Tasks with resource problems
- System identities with access problems
- Persons with awareness deficits
- Devices not physically protected
- Weak infrastructure components
- Assets with risks to mitigate
- Assets with continuity problems
- Assets with CIA issues
- Rules with compliance problems

The calculation of these key indicators is carried out with the help of an aggregation tree and may consist of an absolute number as well as a percentage based on all elements of the linked base set. Therefore, Figure 8.1 shows an example of the visualization of the key indicator for a dashboard. For managers, the percentage and historical data are important for comparison between different departments as well as the temporal change of the metric. The absolute indicates the actual situation of the organization. Not only the top-level indicators can be visualized but also all indicators within the aggregation trees themselves.

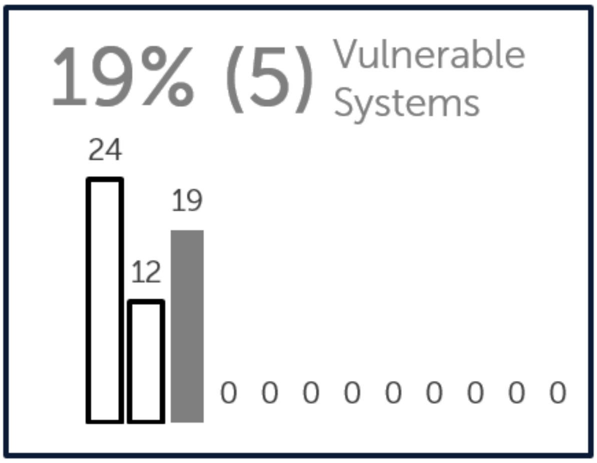

Figure 8.1: *Visualization of indicators*

For each key indicator, an aggregation tree was developed based on the set theory. The following subsections describe each of the trees in detail. The operators of the set theory are used to calculate the aggregated metrics:

- $\cup$ - The union of the connected metrics.
- $\cap$ - The intersection of the connected metrics.
- $\setminus$ - The set difference of the connected metrics.

Every tree can be read from top to bottom and the other way around. To understand the following subsections, Figure 8.2 shows an example aggregation of “Known systems (CMDB)” and “All systems within the infrastructure”. The calculation rule $\setminus$ between them forms the following formula: *Unknown Systems = Known systems (CMDB) \All systems within the infrastructure*. This means that the set different of all systems within the current CMDB and all systems within the infrastructure (e.g. from an IP-scanner) are marked as unknown systems and are then considered as vulnerable (see Figure 8.3).

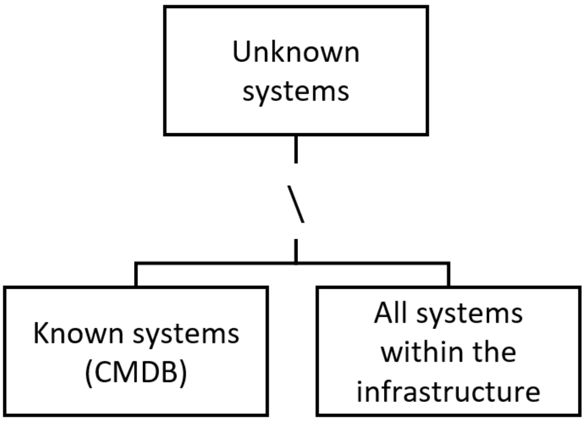

Figure 8.2: *Example of the metrics aggregation*

8.4.3.1 Minimize vulnerabilities

Vulnerabilities in the organizational context are considered to be technical. The given metrics, therefore, consist of technical security metrics. Figure 8.3 shows the different areas of interest when addressing vulnerabilities. A major challenge for organizations is to know all systems within the infrastructure and which of them are being tested or not. The vulnerability-scanning, patching, and software toxicity part are aggregated to the “known weak/vulnerable systems”. Technical vulnerabilities are a critical point of discussion for researchers and practitioners. It is not possible to capture all vulnerabilities within an infrastructure because it might be that the vulnerability is not disclosed to the public. These vulnerabilities are called zero-day vulnerabilities. The critique in monitoring vulnerabilities is that a low vulnerability metric generates a false sense of security for managers. However, not capturing vulnerabilities and constantly monitoring the infrastructure will lead to a higher possibility of compromise as well as an easier way to exploit and therefore increase the risk significantly. Not only targeted attacks on the organization but also random attackers are then able to easily exploit publicly available vulnerabilities.

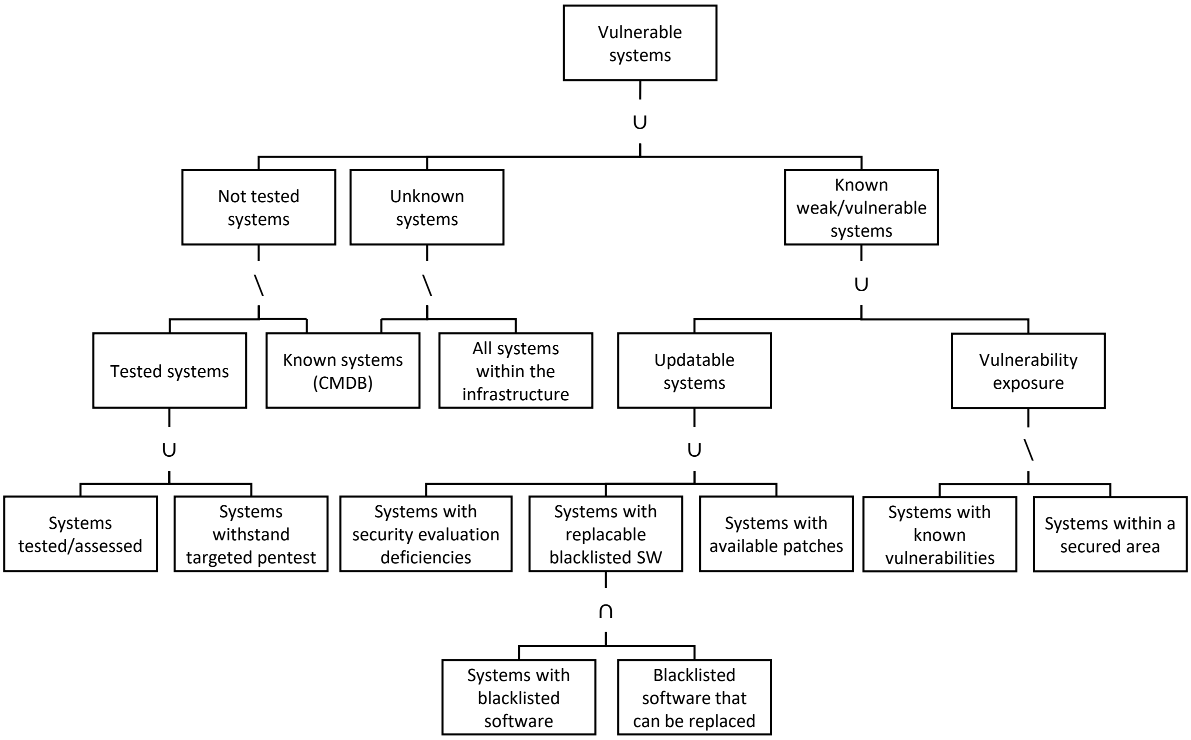
Vulnerable systems
∪
Not tested systems
Unknown systems
Known weak/vulnerable systems
\
\
∪
Tested systems
Known systems (CMDB)
All systems within the infrastructure
Updatable systems
Vulnerability exposure
∪
∪
\
Systems tested/assessed
Systems withstand targeted pentest
Systems with security evaluation deficiencies
Systems with replacable blacklisted SW
Systems with available patches
Systems with known vulnerabilities
Systems within a secured area
∩
Systems with blacklisted software
Blacklisted software that can be replaced

Figure 8.3: *Quantifying vulnerable systems*

8.4.3.2 Optimize resources

Organizations have to act economically. If information security is not a key business of an organization, it is considered to be a cost center. This leads often to insufficient financial resources being made available for security tasks. Therefore, financial resources have to be tracked for the tasks, necessary to protect business information. Not only financial but also qualified staff, as well as time, must be considered for different tasks and including projects. Figure 8.4 shows these different areas and aggregates them into a key indicator for resource problems. Return on security investment (ROSI) is a critical part of quantification. To calculate the metric multiple conditions have to be known and assumed. The advantage is that investment is based on an objective metric that can be understood by the business. The ROSI of a single task is defined as:

$$ROSI = \frac{Annual\ Loss\ Expectancy * mitigation\ ration - Cost\ of\ solution}{Cost\ of\ solution}$$

8.4.3.3 Maximize restrictions to resources

Access control is a subject that is directly related to the information security status of an organization (Diesch/Pfaff/Krcmar, 2020). Protection mechanisms can be as good as they can be. If an attacker has a valid system identity, then these mechanisms are no longer effective. Figure 8.5 shows not just weak system identity keys but also the compliance aspects of system identities and the attempts for compromise.

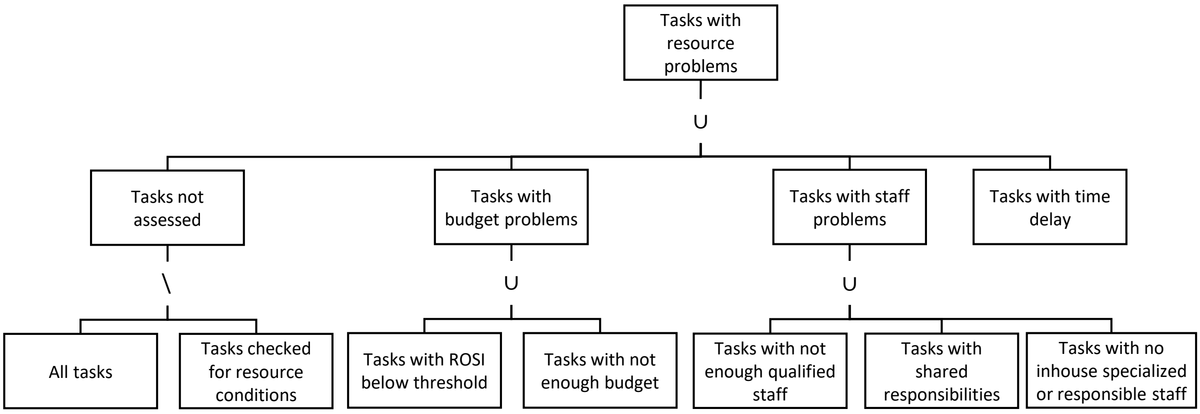
Tasks with resource problems
∪
Tasks not assessed
Tasks with budget problems
Tasks with staff problems
Tasks with time delay
\
∪
∪
All tasks
Tasks checked for resource conditions
Tasks with ROSI below threshold
Tasks with not enough budget
Tasks with not enough qualified staff
Tasks with shared responsibilities
Tasks with no inhouse specialized or responsible staff

Figure 8.4: *Quantifying resource problems*

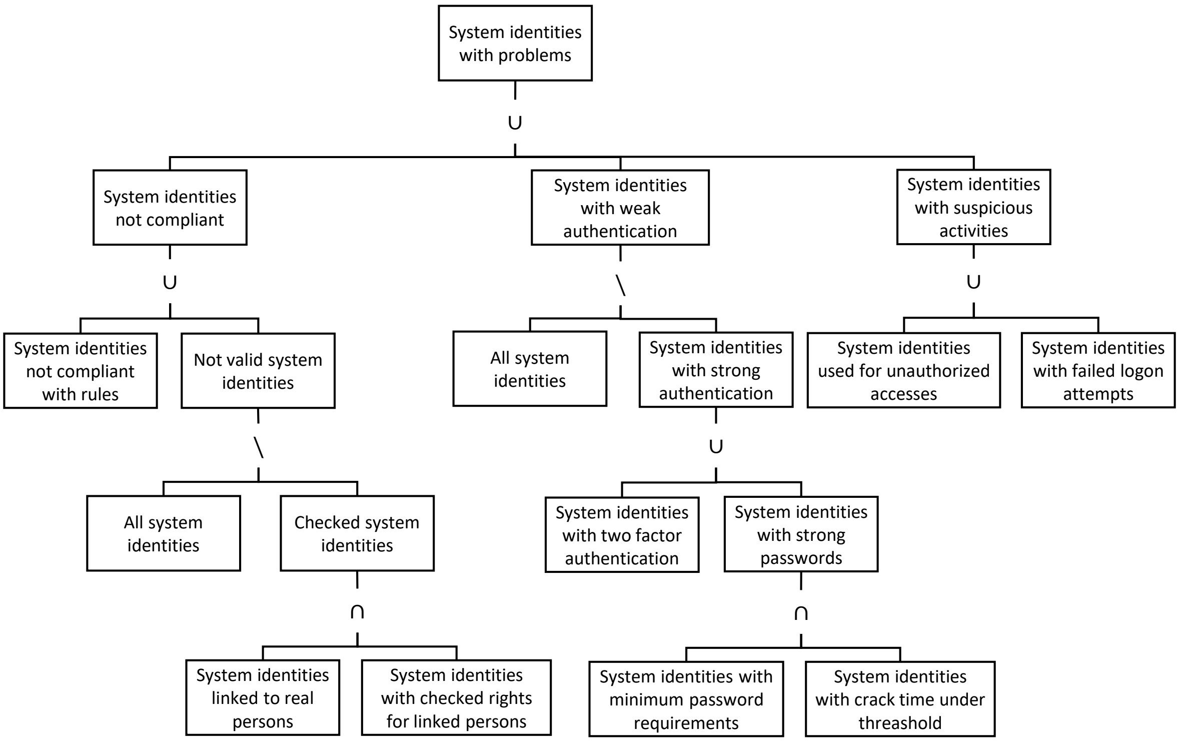
System identities with problems
∪
System identities not compliant
System identities with weak authentication
System identities with suspicious activities
∪
\
∪
System identities not compliant with rules
Not valid system identities
All system identities
System identities with strong authentication
System identities used for unauthorized accesses
System identities with failed logon attempts
\
∪
All system identities
Checked system identities
System identities with two factor authentication
System identities with strong passwords
∩
∩
System identities linked to real persons
System identities with checked rights for linked persons
System identities with minimum password requirements
System identities with crack time under threashold

Figure 8.5: *Quantifying access control*

8.4.3.4 Maximize awareness

Awareness is one of the most important aspects of information security for organizations. People are considered to be the weakest link within an organization. Therefore, Figure 8.6 shows the quantification of different awareness-aspects. Metrics to quantify are included that describe if people are verified by the organization, the people are trained, and the management attention is called.

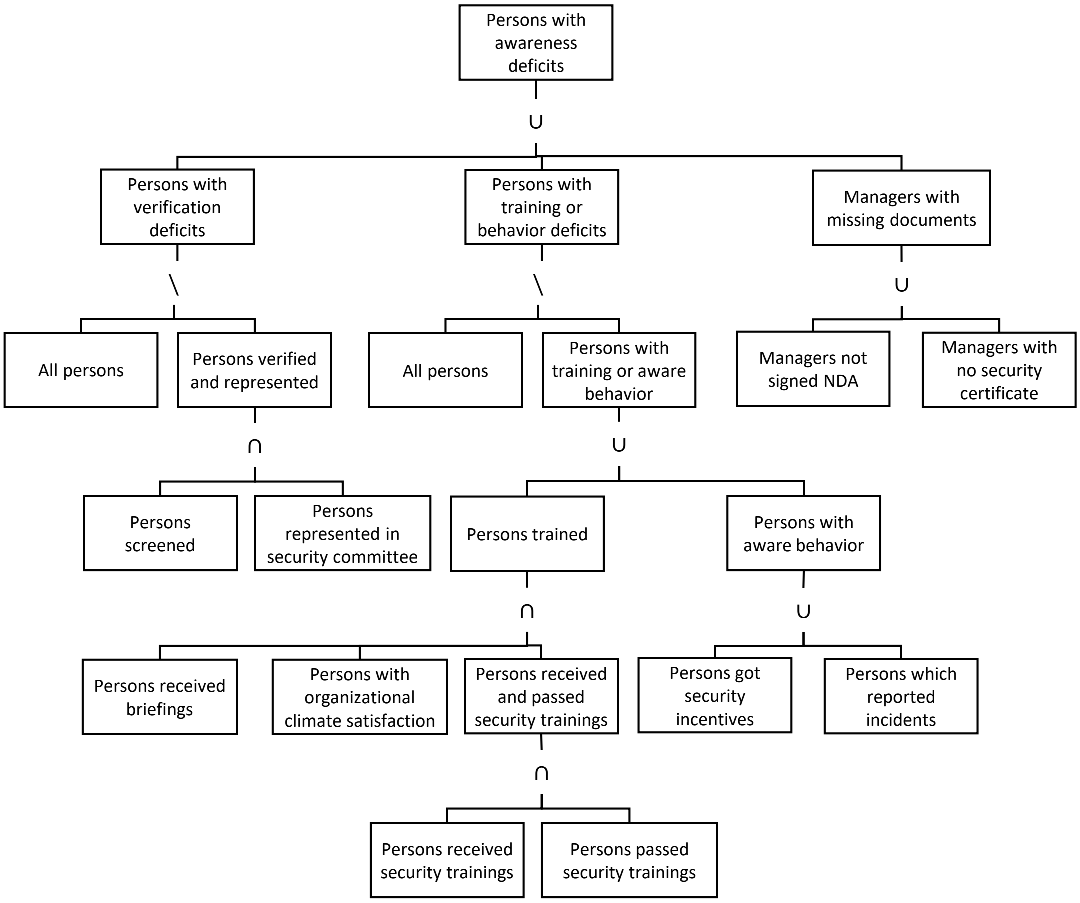
Persons with awareness deficits
∪
Persons with verification deficits
Persons with training or behavior deficits
Managers with missing documents
\
\
∪
All persons
Persons verified and represented
All persons
Persons with training or aware behavior
Managers not signed NDA
Managers with no security certificate
∩
∪
Persons screened
Persons represented in security committee
Persons trained
Persons with aware behavior
∩
∪
Persons received briefings
Persons with organizational climate satisfaction
Persons received and passed security trainings
Persons got security incentives
Persons which reported incidents
∩
Persons received security trainings
Persons passed security trainings

Figure 8.6: *Quantifying awareness deficits*

8.4.3.5 Maximize physical access restrictions

Physical security is not the main part of the information security department of an organization but must be considered by information security decision-makers (Diesch/Pfaff/Krcmar, 2020). Figure 8.7 shows the two main areas of interest. Here, physical devices must be physically protected if their business function is critical. All other devices are marked as being adequately protected. On the other hand, all physical devices must be assessed and marked with criticality. Without the assessment, a decision cannot be made.

8.4.3.6 Maximize infrastructure hardening

Infrastructure monitoring is a difficult task because of new paradigms such as “bring your own device”, “remote access”, and “cloud services”. Figure 8.8 includes infrastructure component (ISC) metrics of infrastructure knowledge, remediation, configuration, ownership, detection mechanisms, and external access. These are typical tasks of the asset management within an organization.

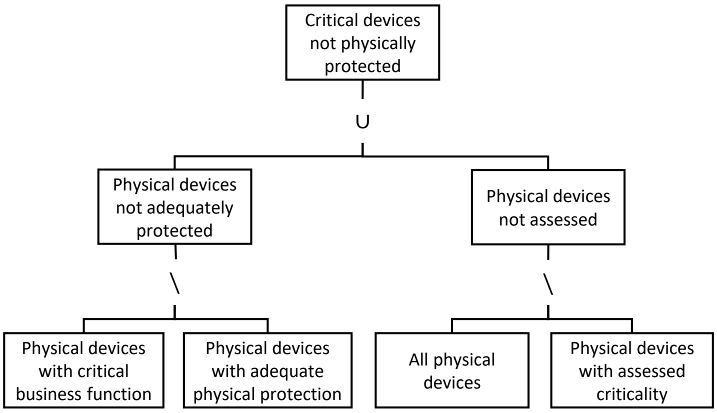
Critical devices not physically protected
∪
Physical devices not adequately protected
Physical devices not assessed
\
\
Physical devices with critical business function
Physical devices with adequate physical protection
All physical devices
Physical devices with assessed criticality

Figure 8.7: *Quantifying physical security*

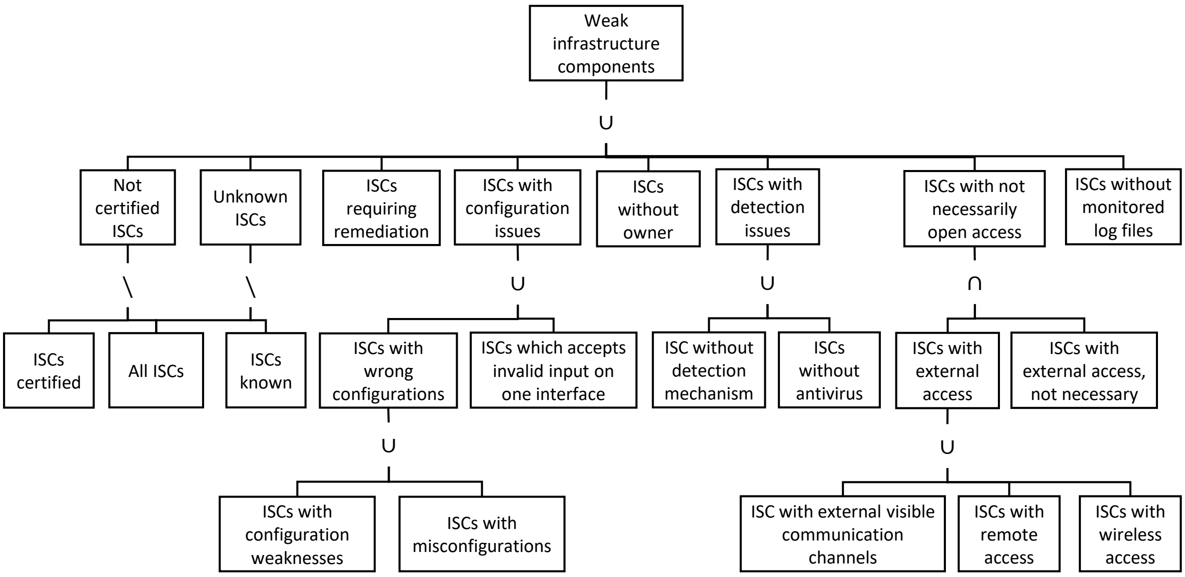
Weak infrastructure components
∪
Not certified ISCs
Unknown ISCs
ISCs requiring remediation
ISCs with configuration issues
ISCs without owner
ISCs with detection issues
ISCs with not necessarily open access
ISCs without monitored log files
\
\
∪
∪
∩
ISCs certified
All ISCs
ISCs known
ISCs with wrong configurations
ISCs which accepts invalid input on one interface
ISC without detection mechanism
ISCs without antivirus
ISCs with external access
ISCs with external access, not necessary
∪
∪
ISCs with configuration weaknesses
ISCs with misconfigurations
ISC with external visible communication channels
ISCs with remote access
ISCs with wireless access

Figure 8.8: *Quantifying infrastructure weaknesses*

8.4.3.7 Mitigate risks based on acceptance level

Information security is most likely based on risk management. Risks are used by organizations to prioritize countermeasures and determine if they are appropriate and cost-effective. In the context of risk quantification, two main focus areas are set out in Figure 8.9. One is the risk assessment of all possible assets. If the risk is not assessed, it could be a high risk and therefore a major concern. The other area is the risk that exceeds a certain threshold. The risk appetite of organizations is the level of risk that can be accepted by an organization. This value is different for each organization and must be set individually for this quantification. "Vulnerable assets can be derived from the other key indicators developed for this dashboard and are highlighted as grey rectangles in Figure 8.9. The vulnerable asset also needs a potential threat and the likelihood of a compromise becoming a risk. These risks have to be evaluated based on the organization's risk appetite.

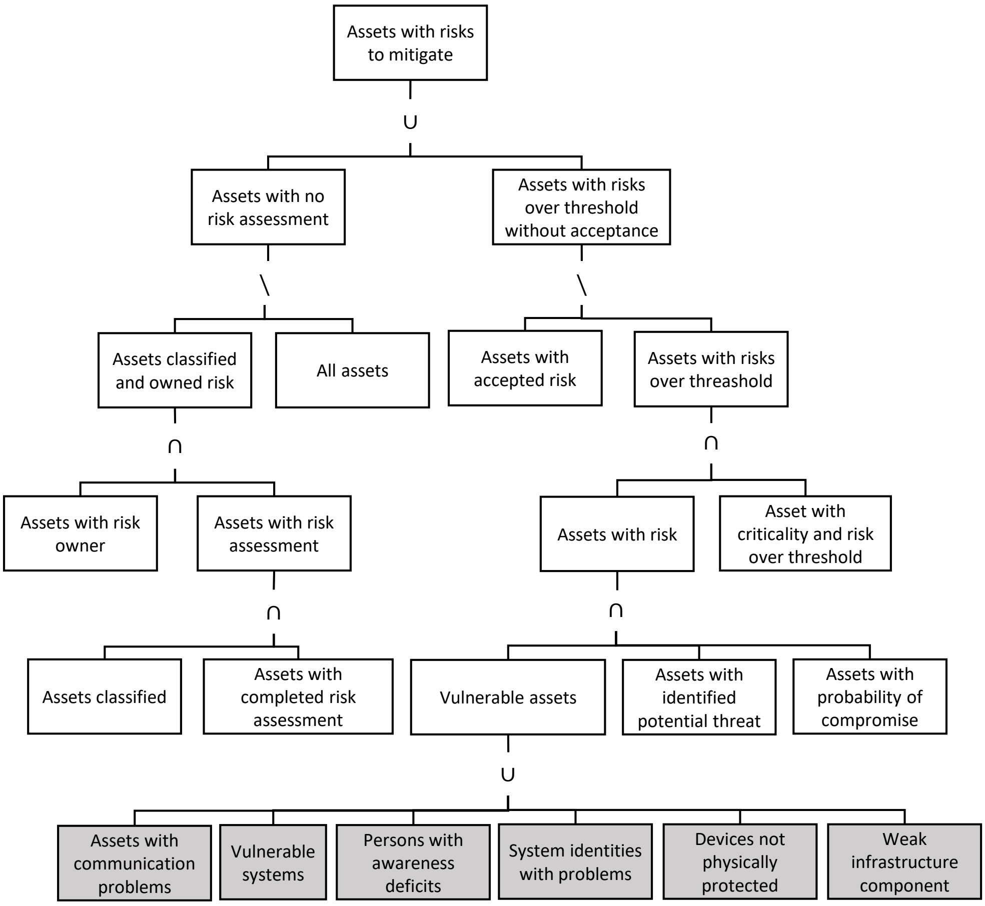
Assets with risks to mitigate
∪
Assets with no risk assessment
Assets with risks over threshold without acceptance
\
\
Assets classified and owned risk
All assets
Assets with accepted risk
Assets with risks over threashold
∩
∩
Assets with risk owner
Assets with risk assessment
Assets with risk
Asset with criticality and risk over threshold
∩
∩
Assets classified
Assets with completed risk assessment
Vulnerable assets
Assets with identified potential threat
Assets with probability of compromise
∪
Assets with communication problems
Vulnerable systems
Persons with awareness deficits
System identities with problems
Devices not physically protected
Weak infrastructure component

Figure 8.9: *Quantifying risks*

8.4.3.8 Maximize the ability to deliver the intended outcome

Continuity is defined as one of the goals to achieve when implementing information security (von Solms/van Niekerk, 2013). Therefore, assets can be reported if the continuity fails, if there is insufficient buffer available, or if assets are not tested for disasters. These are the areas that are quantified in Figure 8.10.

8.4.3.9 Ensure CIA

The CIA triad is also the classical protection goals of information security. Figure 8.11 shows the minimal possibility to quantify aspects of this information security management goal. Availability time of assets, communication encryption, and breaches indicate CIA problems.

8.4.3.10 Maximize rule conformation

Compliance & policies describe requirements that must be implemented and are given internally and externally (Diesch/Pfaff/Krcmar, 2020). Their breaches may be assessed if the management is committed, and if the laws are audited by external organizations. Compliance is necessary if the organization is to receive official certificates or force coun-

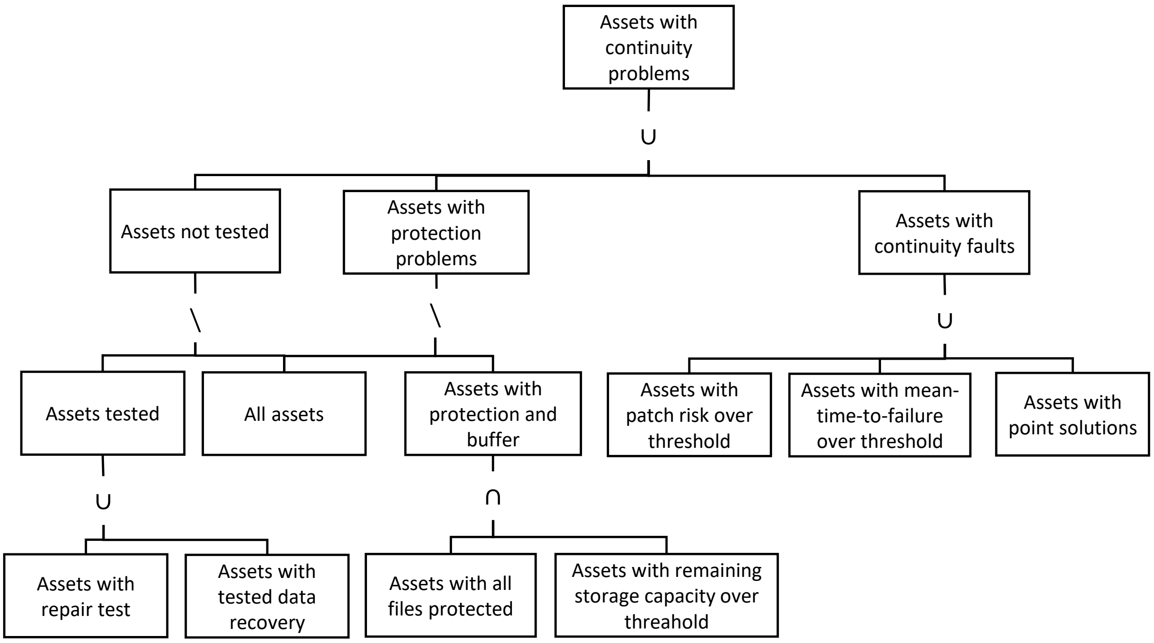
Assets with continuity problems
∪
Assets not tested
Assets with protection problems
Assets with continuity faults
\
\
∪
Assets tested
All assets
Assets with protection and buffer
Assets with patch risk over threshold
Assets with mean-time-to-failure over threshold
Assets with point solutions
∪
∩
Assets with repair test
Assets with tested data recovery
Assets with all files protected
Assets with remaining storage capacity over threahold

Figure 8.10: *Quantifying continuity problems*

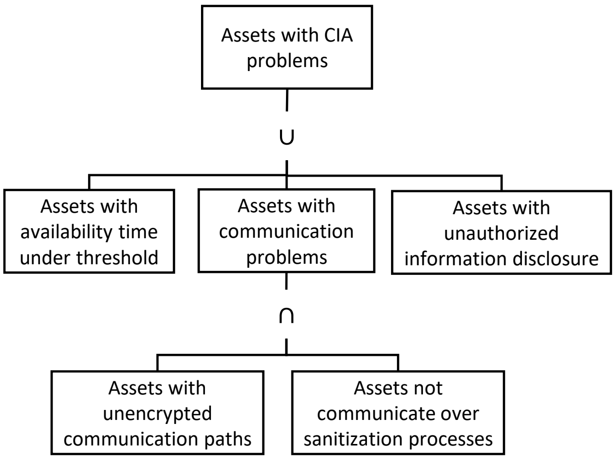
Assets with CIA problems
∪
Assets with availability time under threshold
Assets with communication problems
Assets with unauthorized information disclosure
∩
Assets with unencrypted communication paths
Assets not communicate over sanitization processes

Figure 8.11: *Quantifying aspects of CIA*

termeasures through. The rules without management commitment and enforcement will not improve the information security status itself. Figure 8.12 shows the quantification of these aspects.

8.4.4 Dashboard visualization and recommendations from practice

The information security metrics and the aggregation trees are a valuable tool to gain an overview of an organizations own information security status, report to different management levels, find root causes of problems, cross-compare/benchmark with other departments or organizations, and understand information security aspects.

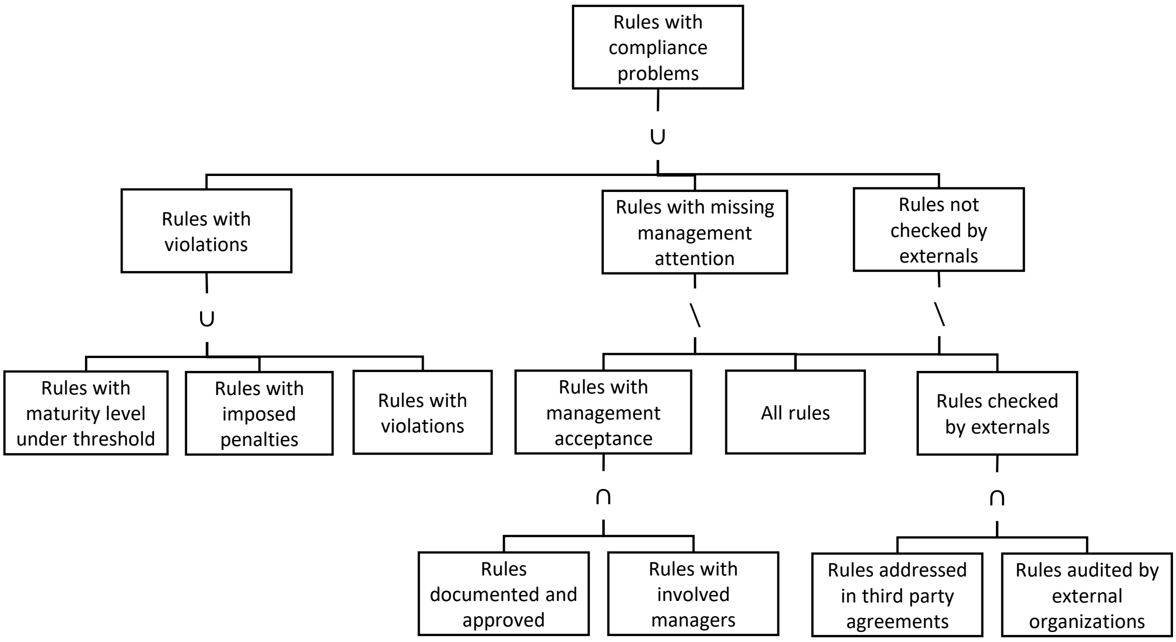
Rules with compliance problems
∪
Rules with violations
Rules with missing management attention
Rules not checked by externals
∪
\
\
Rules with maturity level under threshold
Rules with imposed penalties
Rules with violations
Rules with management acceptance
All rules
Rules checked by externals
∩
∩
Rules documented and approved
Rules with involved managers
Rules addressed in third party agreements
Rules audited by external organizations

Figure 8.12: *Quantifying rule violations*

The information security metrics can be used as the underlying dashboard framework to **obtain an overview of the own information security status**. The main dashboard view will consist of the 10 key information security metrics, the top metric of each aggregation tree. Based on these aggregation trees, different reports with different metric areas can be generated to **different management levels**. This zoom-in and zoom-out feature is not only useful to generate different reporting levels but also to **find root causes of reported problems**. If a large number of vulnerabilities are identified, the aggregation tree offers a range of problem areas and thus different alternatives for intervention. Just a "number of vulnerabilities" do not provide this possibility.

Since all metrics are linked to a base set, they can be compared both with the organization and externally. Classical information security metrics such as the number of vulnerabilities cannot be compared in a meaningful way. An example would be the report of 10 vulnerabilities by two different organizations but one has 10 systems and the other has 1000. A **cross-comparison/benchmark** is possible by linking each metric to the base set. Most small- and medium-sized businesses have problems with the protection of their information assets. They usually do not have enough resources and skilled employees in this particular area where they do not have their main business case. The proposed solution can help them **to understand the different aspects of information security**, what they have to implement, what conditions are required to measure the metrics, and prioritize the protection based on their needs.

Practitioners from the workshop also see the current problems of (1) too many metrics to gain an easy-to-understand overview of the current information security situation, (2) metrics are not actionable, (3)cmetrics are not tractable, and (4) do not provide comparability from design. There is also the possibility that metrics (5) may be manipulated, or even that partners, clients, or departments may simply provide the metrics they want to deliver. Often, the individual conditions of the metrics (e.g. the number of systems) are not clear in practice. From the management perspective, a metrics aggregation must ensure that the important, critical information is given top priority. The problem in practice is: The higher the abstraction level, the more difficult it is to deliver metrics that are understandable and easy to use. Often, many people responsible for security are not security experts and are having trouble understanding the risks presented or metrics themselves. The proposed solution in this research reveals several advantages that the experts have identified to overcome the described problems:

- *Understandability:* The practitioners consider the overall approach as "understandable and feasible". The first impression of the trees was that the trees have too many layers. But, after looking at these, the expert said: "Maybe it is the way how it is displayed, that it looks more complicated than it is." The consensus was that the trees can be a very useful tool to present metrics to the management in a meaningful and comprehensive way. Even large organizations that already deal with existing metrics and have a well established information security assessment can use the trees for this purpose to improve the understandability.

- *Viable as a target picture:* The conceptual dashboard is useful for gaining a target picture of what needs to be covered in conjunction with the information security of organizations. An organization can look at the current situation and check the availability of the necessary data within the trees. If the organization can just cover a part of the trees, they would realize which parts are missing and need to be looked at. This target picture is useful to get full transparency of the information security status of the organization. The trees not only show positive areas but also areas that are unclear for information security management.

- *Provide actionable results:* The hierarchies make the metrics actionable because they provide an insight into possible areas that can be improved. A metric from literature and often used in practice - "number of vulnerabilities" - does not provide management with opportunities for improvements. To improve this metric, the people responsible for information security decisions have to find the root cause of the underlying metric. Not only the cause but also the conditions under which this metric was calculated must be considered. Questions such as how many systems were tested, which systems have vulnerabilities, or are the vulnerabilities caused by an old patch state remain unanswered. The proposed dashboard provides areas for improvement and as one expert said: "It is obvious how to improve the given metrics." The experts also liked the possibility of pruning the metrics. A top-level manager can just look at the top-level indicator and find root causes if the metric is not good enough for him. "The tree shows where to act now".

- *Simplicity:* The visualization is simple (expert statement: "simple in a good way") and easy to understand. At the same time, the trees are comprehensive.

- *Deliver the right information:* The trees are useful for delivering different tree hierarchies to different levels of management of the organization. Therefore, not only the top-level management can benefit from this dashboard. It is not possible to hide information between different levels of management in the organization. Also, "the important information comes through and is displayed to the top". Information security managers are concerned with the most critical information. This information is normally lost in classic key metrics. The proposed dashboard provides that the critical information goes to the top of the dashboard and that corrective actions can be taken by the managers.

- *Comparability:* The metrics are comparable by design. Further normalization is not required because all metrics are related to a base set that can be used to display percentages. This normalization provide comparability.
- *Automation:* Experts suggest the development of an automated system for collecting the necessary data and presenting the data to information security management. This would also overcome some challenges with regard to the proposed dashboard solution that are described in the next paragraph.
- *Feasible for other areas:* The proposed solution is not only feasible for the assessment of internal information security risks but also for information security and risk assessments for clients. Therefore, the proposed metrics and the underlying areas described should also be considered when assessing or consulting client's risks in the area of information security.

The experts also see some challenges regarding the use of the proposed conceptual information security assessment dashboard:

- *Data foundation and collection:* The proposed conceptual dashboard needs a well-established database to instantiate the trees. The possibility of collecting the data might depend on organizational size and capacity. "Some organizations do have all the information at hand, others, mostly small- and medium-sized businesses, don't." Therefore, the experts believe that it might be difficult for small- and medium-sized enterprises to collect all the necessary data with an acceptable effort. To overcome this challenge, it would be beneficial to develop a system that automatically collects all the necessary data.
- *Organizational commitment:* To implement the proposed conceptual dashboard, the entire organization must commit to the methodology. There is a possibility, that some organizations have already begun discussions and conversations on the issue of information security assessment. These conversations would be interrupted by presenting a new approach to them.
- *Deep understanding:* Even for a professional, it takes a while to think through all the trees. The pruning of the trees does make absolute sense because it ensures that parties involved are not overwhelmed at first sight.
- *Confidential information:* The metrics within the proposed solution "cannot be discussed". This leads to the assumption by the experts that other companies would not share this information with others. The metrics show you exactly the information security status of an organization. It would be very difficult to share these data in order to benchmark them.

8.5 Discussion and directions for future research

From a management perspective, this research proposes a conceptual information security assessment dashboard. The results were obtained based on existing work, which includes information security management success factors, information security metrics, and an information security metrics aggregation method. Based on the design-science methodology, 10 key indicators with their aggregation trees were developed. The tree structure with metrics and indicators are forming the dashboard for information security managers. Experts in the field (a focus group) evaluated and refined the dashboard.

Key indicators are useful for information security experts and business managers to gain an overview of the measured constructs. Normally, these indicators are calculated based on mathematical functions and numbers. If a manager wants to make a decision based on this key indicator, the alternatives to improve the indicator is not given by the number. Also, the information aggregation theory (see Section 8.2.4) describes that detailed information is lost within the calculation, which can reduce decision quality. The proposed conceptual dashboard with a zoom-in and zoom-out feature reveals different options for action as well as hold the underlying information of the key indicator. This function not only holds the original information but can also serve as a reporting function for other information security management levels. The aggregation of the metrics forms thematic focus areas and indicators of these areas. The monitoring of areas is provided by different views on the dashboard. Problems presented by the information aggregation theory can be reduced effectively.

The conceptual dashboard also serves as a means of mitigating the disadvantages revealed by the information asymmetry and information overload theory. The dashboard provides a standardized way to assess the information security status of an organization. This results in the avoidance of information asymmetry within teams and organizations and thus the reduction of possible manipulations. Manipulations could be the reporting of one's defined metrics to higher-level managers in order to gain personal advantage from it. The pruning function of the dashboard, which provides different views, results in a reduction of information and, in consequence, the avoidance of information overload. Only the necessary information can be presented to specific persons within different areas of information security. The pruning of the information should improve decision quality by reducing the effect of information overload. This was also the feedback from experts in the field: that the proposed solution provides the necessary information.

The proposed dashboard has multiple practical contributions. The dashboard can be used directly to support the development of an information security monitoring and risk assessment program. It provides comparable metrics that are useful for visualizing problem areas and explains the underlying aspects of the different information security concepts. This dashboard sets out the requested link between technical information security indicators and information security management objectives. With the help of this dashboard, the gap between the technical metrics described in different standards such as NIST 800 or ISO/IEC 27000 and the understanding from a management perspective could be closed. The use of the conceptual dashboard can be extended to serve as a target picture in order to gain full transparency over the information security status of the own organization. Responsible persons who are necessarily not information security experts (mainly in small- and medium-sized enterprises) would benefit from this work. The experts said that the metrics within this solution "tells a lot about how the security looks like, which is the perfect view that you as a security responsible need on your company."

Not only one's information security status can be monitored and assessed. Some organizations require their suppliers and customers (clients) to comply with specific information security standards. For example, insurance companies ask their clients to quantify their information security with a self-assessment to calculate the specific insurance charges. Such organizations could use the proposed dashboard. It explains exactly how to quantify the information security aspects and which data are necessary. Also, the results are compared to others, which allows them to be benchmarked. Further information security certificates or public benchmarks based on this dashboard could serve as advertising tools for organizations. At a time when "cloud services" and "outsourcing" are a day-to-day business and the information security aspect of these services is very high, the provision of these data to potential customers could serve as a decision support and quality criteria.

Each research has its own limitations. The first result of the conceptual information security assessment dashboard was developed solely by the authors and is based on previous research. Despite the evaluation based on a workshop with experts in the field, the results could be biased on the presentation of the first results. Also, the evaluation was carried out with experts from one organization, and this could have led to bias in the direction of the organization's culture, experiences, and meanings. However, to the best knowledge of the authors, this research proposes the first comprehensive conceptual information security assessment dashboard from the information security management perspective of an organization.

Future research could evaluate the conceptual information security dashboard through multiple studies with other organizations and practitioners and refine the proposed results. The conceptual dashboard can be used as a basis for a technical implementation of this dashboard to automatically assess the information security status of an organization. This was also asked by the practitioners within the workshop: a tool that automatically collects and visualizes the necessary data from the organization's infrastructure as a technically implemented dashboard. With this instance, multiple studies are possible. Future research could focus on the effectiveness of different countermeasures from standards and best practices, the impact on the decision-making quality (decision theory) of information security managers, the comparison of different states of information security, or the development of a recommender system for information security decisions.

8.6 Conclusion

Information security management is a major concern for organizations. To continuously improve the information security status of an organization, the assessment of the information security status is necessary. Multiple standards and best practices such as ISO/IEC 27000, NIST 800, and ISF suppose metrics. Such metrics, however, do not measuring the minimum information security information needed and lack the connection to the objectives of information security management. As a result, literature and practitioners requested reporting standards and dashboards for the information security status of an organization.

This research proposes a conceptual dashboard to assess the information security status of an organization from a management perspective. The dashboard was developed using the design science research approach and the information security metrics aggregation method. Also, information security management success factors, as well as the available metrics, were used to develop the suggested dashboard. An evaluation was carried out with the help of a workshop by experts from a leading global organization.

The dashboard consists of 10 key indicators for the information security management level. Each key indicator is based on a metrics aggregation tree and thus supports a zoom-in and zoom-out feature to better understand the information security aspects, find root causes in the event of appropriate changes, show action alternatives for decision-making, and support cross-comparison with other organizations. Also, the dashboard reduces the inconveniences of multiple decision theory constructs. Information overload, information aggregation and information asymmetry effects can be minimized to improve the decision-making of information security managers.

Part C

Summary of Results and Discussion of Implications

9 Summary of Results

The development of a conceptual information security assessment dashboard for organizations from a management perspective is based on different challenges and gaps in the literature. These challenges are taken by the five publications embedded in this thesis. The main results of these publications are summarized in the following itemization as well as illustrated in Table 9.1.

- The first publication (P1) uses a state-of-the-art literature review to develop a research agenda for the challenging task of assessing the information security status of an organization. First, the publication reveals the terms Information and Communication Technology Security (ICT), Information Security (IS), Cyber Security (CS), and Cyber Resilience (CR). These terms are delimited to provide a common understanding for future research. The thematic classification of past literature suggests the main research streams "information security management", "information security measurement", "human behavior", and "practical frameworks". The different research streams are the basis for the discussion of shortcomings in past literature which leads to a proposed research agenda. A major shortcoming was the missing comprehensive view on information security assessment and the definition of an information security status. To address this shortcoming, the development of a comprehensive view of information security from a management perspective with the development of metrics that measure this view was proposed.

- Publication two (P2) treated the challenge of a missing comprehensive view of the information security phenomenon within organizations and the common understanding of the topic. First, 12 factors that influence information security managers' decisions were explored with the help of a literature analysis, an open-axial-selective coding, and a semi-structured expert interview. The interview series also revealed interdependencies between the factors to finally propose a comprehensive model of information security management factors for the information security of an organization.

- Publication three (P3) is motivated because metrics in literature are separately studied and not goal-oriented. Therefore, these metrics are not useful for serving as management indicators. A literature review in combination with the Goal-Question-Metric approach was used to propose a list of useful metrics that are linked to the management factors of P2. Metrics within this publication are not studied separately but in a broader context and therefore clustered by their measurement objective. The results suggest that not all factors that have an impact on management decisions are quantifiable.

- Publication four (P4) is about the challenge of how to develop and/or aggregate information security metrics to meet management requirements. These are, that information security metrics have to be goal-oriented, actionable, traceable, and comparable. Also, current metrics are not understandable, clear, and useful. Therefore, this publication provides a general method to aggregate information security metrics to meet these requirements. The method was developed with a simulation of an instance as well as a semi-structured expert interview. The publication suggests the use of the method to develop an information security measurement/assessment standard for information security managers and employees.

- The last publication (P5) is challenging the need for an information security dashboard for organizations. Management decisions rely on indicators that are reported to them. Different phenomena influence decision-quality such as information overload, information aggregation effects, and information asymmetry. The publication proposes a conceptual information security assessment dashboard for information security managers of an organization that minimize the negative effects of these phenomena to decision quality. The dashboard proposes possible areas for taking actions and improve the information security status of an organization. Also, the dashboard allows it to push important information through the top while other metrics do not highlight important information security weaknesses to the relevant abstraction level.

No.	**Title**	**Findings**
P1	Prerequisite to Measure Information Security - A State of the Art Literature Review	• Delimitation of the terms Information and Communication Technology Security (ICT), Information Security (IS), Cyber Security (CS), and Cyber Resilience (CR) • Categorization of literature in the information security metrics domain and identification of the research streams. • Description of current challenges and recommendations for future research in the form of a research agenda.
P2	A comprehensive model of information security factors for decision-makers	• Identification of 12 factors that influence information security managers' decisions. • A ranking of the factors that are important for the actual status of an organizations' information security. • Identification of interdependencies between the factors to present a comprehensive model of these.
P3	SoK: Linking Information Security Metrics to Management Success Factors	• Identification of available information security metrics in the literature. • Link of available information security metrics to information security management goals. • Not all factors that influence decision-making are quantifiable.

P4	Reducing Complexity - A Method to Aggregate Security Metrics	• A method to aggregate information security metrics to key indicators while generating understandable, actionable, and comparable results for the management of an organization. • A simulation of an instance indicates a better performance of the resulting key indicator (vulnerable systems) than available metrics in the literature (number of vulnerabilities).
P5	A Conceptual Information Security Assessment Dashboard for Organizations	• The development of 10 key indicators for information security managers based on 83 metrics. • A dashboard that meets information security managers' requirements and supports decision-making. • Relevant areas and possibilities for decision-making of organizations in the information security domain.

Table 9.1: *Summary of Results*

10 Contributions of the Thesis

The results of the embedded publications (P1-P5) and therefore this thesis contribute to different existing research streams and theories (see Section 10.1) but also have practical implications (see Section 10.2) that are discussed within this Chapter.

10.1 Contributions to Theory

A summary of all theoretical contributions are illustrated in Table 10.1 followed by a detailed explanation of them ordered by the research streams.

Research stream	**Topic - Contribution**
Information security research	**Terms** - Definition and delimitation of the terms Information and Communication Technology Security (ICT), Information Security (IS), Cyber Security (CS), and Cyber Resilience (CR). **Security management overview** - Provide a comprehensive view of information security factors and their interrelations that influence decision-making of managers. **Dashboard** - Provide a detailed information security assessment dashboard that describes areas of interest and their sub-aspects of information security as a complex phenomenon.
Information security assessment	**Synthesizing literature** - Consolidation of different research streams and shortcomings in past literature. **Management objectives** - Provide clear management objectives and a rating of their importance according to expert opinions. **Default metrics** - Provide a comprehensive set of metrics and their link to management objectives to cover management requirements. **Metric abstraction** - This thesis contributes to the shortcoming of not goal-oriented metrics in literature by providing a method to aggregate technical security metrics to abstract them to key indicators. **Dashboard development** - How to design and construct a suitable dashboard in the context of information security assessment. **Risk assessment** - This thesis provides metrics that support all steps within the risk management process.

Decision theory	**Decision uncertainty** - Reducing uncertainty by (1) improving the understandability of information security as a complex phenomenon and (2) provide action alternatives for information security managers. **Information overload** - Reducing information overload by aggregating information security metrics to a management level. **Information asymmetry** - Avoid information asymmetry by providing a transparent view of the information security situation for all groups and business members. **Information aggregation** - The thesis proposes a methodology that allows information aggregation without loosing the original information.

Table 10.1: *Summary of contributions to theory*

Information security research

Information security research is divided into several research streams such as information security management, policy compliance, or technical information security issues. A substantial contribution presented in publication one (P1) is the definition and delimitation of the four different terms in relation to themselves: Information and Communication Technology Security (ICT), Information Security (IS), Cyber Security (CS), and Cyber Resilience (CR). The definition of the terms and their usage in practice contributes to research by extending the work of (von Solms/van Niekerk, 2013). The uniform usage of the terms would help to differentiate between research areas and their focus. The rise of CR within past literature indicates that information security within an organization's context can not be limited on assets that have information stored or transmitted directly but also on all assets related to this information. Information security risk management literature proposes the categorization of assets based on the value of the stored information to the business (Fenz et al., 2014; Gritzalis et al., 2018). Taking the definition of CR into consideration, the information security risk management should also analyze the relation to valuable information as well as their position within the business delivery chain. This analysis leads to possible higher criticality or value than only looking to the asset and the stored information itself and, in consequence, should have a higher security standard.

The shift from a technical to a management perspective and thus the shift of responsibility for information security within organizations (Soomro/Shah/Ahmed, 2016) lead to a change of the research focus in the literature. For managers, it is important to consider all necessary factors to make effective decisions and mitigate threats (Coronado et al., 2009). Therefore, the work of multiple authors (Kraemer/Carayon/Clem, 2009; Norman/Yasin, 2013; Soomro/Shah/Ahmed, 2016; Horne/Maynard/Ahmad, 2017) requested a comprehensive view of information security. D'Arcy/Herath (2011) also described that such accurate models of the information security problem are not in place and a gap in the literature. The second publication of this thesis (P2) contributes to the described gap as well as the understanding of information security in general by providing a comprehensive model of information security management factors that influence decision-making in an organizational context. Not only the factors but also their interdependencies are provided and build a theory that explains relationships and factors for information security decision-making. Past research in the information security domain within highly ranked journals focusses mainly on business continuity management, information security governance, and information security incident management (Silic/Back, 2014). The results of P2 questions the focus of past literature based on empirical evidence that factors like business continuity, security management, and compliance & policy are less important for the information security status of an organization than key factors such as vulnerabilities, resources, awareness, access control, and physical security.

The core result of this thesis - the conceptual information security assessment dashboard - extends the understanding of important aspects of information security with their relationship on different levels of abstraction. A question on which sub-aspects are important when speaking about information security aspects such as vulnerabilities, risks, awareness, or physical security are illustrated and proposed by the results of publication five (P5). Dzazali/Sulaiman/Zolait (2009) suggested that future work "should not just focus on technology but also the people, processes, and business goals that support the technology". The results of P5 addresses this gap in serving as a detailed description of important areas of interest with their sub-aspects and the relationships between them in order to understand information security as a complex phenomenon. Also, the result contributes to a large research community that asks for information security dashboards in general (Dogaheh, 2010; Maier et al., 2017; Al-Darwish/Choe, 2019; Tewamba et al., 2019) by providing a first comprehensive dashboard that meets requirements from the literature (see Savola/Heinonen, 2011).

The understanding of information security with the different aspects and factors is the first step towards the topic of assessing information security in detail.

Information security assessment

Research in the field of information security assessment pointed out the need for intensified research in measuring and monitoring information security (D'Arcy/Herath, 2011; Crossler et al., 2013; Fenz et al., 2014; Sommestad et al., 2014). Publication one (P1) contributes to this field by synthesizing the diverse literature to research streams and propose different gaps in research as well as a research agenda. P1 provides a foundation knowledge of information security measurement, the different terms used in the literature, and the description of the different areas of research. Future research can be captured more easily and the context of these articles are more clearly based on the proposed streams.

A major challenge in the area of information security assessment using metrics is that the metrics suggested in the literature are not goal-oriented (Leon/Saxena, 2010; Rudolph/Schwarz, 2012). This problem is present because current information security metrics are too technical (Boehm et al., 2018) and the goals of the information security management are not clear (Leon/Saxena, 2010). The results of P2, P3, and P5 suggest a list of high-level goals that are important for an information security manager of an organization. The goals are empirically validated and consist of a detailed description from theory, practice, and problems when dealing with this goal. The results indicate that certain goals - named key security indicators - are more important than others in ensuring a basic level of information security within organizations. The challenge of providing metrics that are useful for the management of an organization, and are not purely technical, is addressed by providing a method for aggregating information security metrics in P4, as well as detailed metrics suitable for measuring the goals set in P5. These results contribute to the literature by addressing the gap of providing metrics useful for managers' needs and do not support their decisions or adequately represent the value of security activities, stated by multiple authors (Hayden, 2010; Jafari et al., 2010; Chai/Kim/Rao, 2011; Bayuk, 2013; Fenz et al., 2013; Azuwa/Sahib/Shamsuddin, 2017). The result of P4 suggests that the information security assessment has to be pessimistic rather than optimistic. This means: If an aspect is not tested, it is considered to be negative. For instance: If a system is not tested, it is considered to be vulnerable. Therefore, P4 states that despite the previous literature, the assessment of information security had to assume negativity or bad behavior.

The development of information security metrics and measurement of information security is at an early stage of research and is still quite underdeveloped (Savola, 2009; Savola/Heinonen, 2011; Zalewski et al., 2014). P3, P4, and P5 contribute to this early research stream in multiple ways: (1) Provide a list of metrics linked to management goals, (2) a method to aggregate information security metrics, and (3) a comprehensive view on metrics and their aggregation in form of a conceptual dashboard. The results also contribute to solving a challenge mentioned in the literature that metrics are studied separately in the past (Tashi/Ghernaouti-Hélie, 2008) and available metrics do not cover the minimum security requirements of organizations (NIST, 2008). A common criticism of available metrics are, that they measure the effective implementation of processes rather than the actual state of the information security status itself (Bayuk, 2013). The results of P3 and P5 confirm this statement and suggest metrics that actually measure the information security status itself.

Dashboards are "regarded as a data-driven decision support system" (Yigitbasioglu/Velcu, 2012). They are a common tool to present the results of an information security assessment to different levels of management and thus interesting for research. Past research of dashboards that deal with aspects of information security focus on visualization patterns (McKenna et al., 2016), the influence of mental models to dashboards (Maier et al., 2017), or requirements to possible dashboards (Savola/Heinonen, 2011). P4 and P5 contribute significantly to the research of dashboards in the construction phase as well as to the provision of a comprehensive dashboard for information security assessment. The method to aggregate information security metrics - the main result of P4 - suggests the use of the method in order to generate dashboards by meeting the requirements of Savola/Heinonen (2011). P5 shows, how a dashboard can be conceptualized before implementing it into practice. Dashboards need to be evaluated based on their design features (Yigitbasioglu/Velcu, 2012). In this context, the suggested results extend the understanding of dashboard design and construction.

The main objective of this thesis is the development of a conceptual information security assessment dashboard. This objective emerges from the research gaps of missing models of the security problem (D'Arcy/Herath, 2011), lack of the measurement of aspects of information security (Fenz et al., 2014), lack of understanding the complexity of information security (Willison/Backhouse, 2006), and the lack of having a comprehensive view of information security (Soomro/Shah/Ahmed, 2016). Summarized, security metrics in the past are not connected to existing information security models or are not aligned to management goals and strategic objectives (Bayuk/Mostashari, 2013; Collier et al., 2016; Pendleton et al., 2017; Azuwa/Sahib/Shamsuddin, 2017). P5 supports this statement and contributes to research by providing the first comprehensive information security assessment dashboard. The development of the dashboard uses existing metrics (P3) and aggregates them with a method (P4) in order to connect them to an existing information security model (P2).

Information security risk management is also affected by this thesis because information security assessment is a major task within the process. P2 and P5 indicate that risks are a major factor that influences information security decisions. Therefore, the suggested dashboard also includes the quantification of information security risks based on the other factors within the result of P2. The proposed solution of P5 contributes to the understanding of the aspects that are important for all tasks within the risk management process - namely risk identification, risk analysis, risk control, and risk monitoring (Krcmar, 2015).

Information security assessment and risk management are tools that serve as a basis for making decisions. Therefore, this thesis also contributes significantly to decision theory.

Decision theory

Behavioral decision theory deals with uncertainty and the use of heuristics when making decisions. This applies strongly for decisions in the information security field because there, managers make decisions often by their experience, judgment, and their best knowledge (Chai/Kim/Rao, 2011). P2 extends the understanding of factors and their interrelations and therefore illustrates possible consequences of decisions that influence one of the proposed factors. The uncertainty is also related to the possibilities of action. Straub/Welke (1998) pointed out that risks can be reduced more effectively if managers are aware of the full range of controls available to them. P2 and P5 reduce uncertainty by providing an overview of possible action alternatives on different management levels. These alternatives are “ranked” by indicating weaknesses of the information security status with the help of metrics and indicators. Decision theory is defined as “a powerful tool for providing advice on which management alternative is optimal given the available information” (Polasky et al., 2011). The discussed contribution fits in the definition and improves the possibility to reduce uncertainty, increase available information, and present weighted action alternatives to information security managers.

Information overload is a phenomenon that reduces decision-quality if more information is available than necessary. Past literature proposes up to 900 metrics (Herrmann, 2007) to measure aspects of information security and managers in practice also reported a large number of metrics within reports (Boehm et al., 2018). This amount of information is likely to trigger information overload at a management level. P3, P4, and P5 suggest metrics and a method to aggregate them in order to reduce the information to the needed amount of data on a management level. P4 contributes to the reduction of information overload in general by showing a method to accomplish this reduction while producing usable, understandable, and traceable results. P5 suggests a dedicated instance to reduce personal information overload for information security managers while tackling the challenge of computer-generated reports (see Section 2.2).

Information asymmetry is the concept of imbalanced information between group members or groups (see Section 2.2). The research of information asymmetry showed that the manipulation tendency and the effectiveness of these manipulations are highly increased when increasing information asymmetry (Malekovic/Sutanto/Goutas, 2016). P5 provides a standardized way to quantify aspects of information security and suggests a dashboard for transparency. Empirical evidence is given, that this increases the overall understanding of information security within organizations. Also, the information is available for all stakeholders and hiding and manipulation should not be possible by a standard for information security assessment. The results show a way to reduce information asymmetry and minimize manipulative tendencies.

Information aggregation is the "combination of information according to some type of integration rules" (Speier-Pero, 2019). The research of this phenomenon is often a part of information overload by being the opposite - information underload. By reducing information, the information is not available to take into consideration when making decisions. P4 and P5 suggest a method and a specific instance of performing information aggregation by keeping the original information unchanged and traceable backward (to the beginning of the information integration rule) for more detailed investigation within the decision-making process.

Overall, the results of P2, P3, P4, and P5 contribute to decision theory by providing a suggestion of how the negative effects of information overload, information aggregation, and information asymmetry can be reduced by minimizing uncertainty and providing a full range of action alternatives.

10.2 Contributions to Practice

Table 10.2 includes an overview of the contributions to practice of this thesis. In the following, a detailed explanation of them ordered by the topic is provided.

Topic	**Keyword - Contribution**
Information security understanding	**Management overview** - Information security factors and their interdependencies provide a high-level understanding for experts and non-experts that are responsible for the information security of organizations. **Organizational shortcomings** - The solution illustrates the needs and shortcomings of an organization regarding information security. **Argumentation basis** - By using the proposed solution, it supports as an argumentation basis for necessary actions to the business management. **Practical use** - The thesis shows evidence that the results are understandable, easy to use, and feasible for practitioners.

Information security metrics	**Possible metrics** - The thesis provide a comprehensive list of information security metrics for organizations. **Metrics with objectives** - The thesis illustrate the management a link to the different management objectives for each metric. **Continuous improvement** - The proposed results provide the management a basis to measure and control the continuous improvement of an organizations' information security.
Metrics aggregation	**Aggregation methodology** - The information security metrics aggregation method can be used to aggregate existing metrics and measurement approaches in organizations. **Understanding of metrics** - The aggregation improves the understandability and usefulness of existing metrics to cover management needs. **Dashboard development** - The results enable organizations to develop comprehensive, understandable, and traceable indicators for their dashboards.
Target picture	**Information security transparency** - The proposed dashboard can serve as a target picture to gain full information security transparency. **Necessary data** - The solution illustrates which data is necessary and what areas of interest need to be addressed by an organization. **Evaluation instrument** - The results can serve as an instrument whether an organization addresses all aspects and which countermeasures are effective.
Decision support system	**Dashboard** - The main result of this thesis is a dashboard that serves as a decision support system for information security managers in practice. **Comparison** - The metrics are designed to support comparisons between organizations and organizational departments. **Illustrate technical shortcomings** - The result enables a trace back to the root causes of information security shortcomings from key indicators downwards. **Action alternatives** - The tree structure of the dashboard contains action alternatives directly to managers and illustrate their effects on the related objective. **Different abstraction layers** - The dashboard provides sub-trees for different levels of management or even functional departments.
Benchmarking	**Key indicators** - The key indicators of the solution are possible benchmarking tools for cross-organizational comparisons. **Quality indicator** - The results could serve as information security quality indicators for providers to customers.

Table 10.2: *Summary of contributions to practice*

Basis for information security understanding in organizations

Information security in its complexity is not easy to understand even for information security technical experts. P2 can be used for gaining an overview of different key factors and how they are related to each other on a highly abstract level. The result of P5 includes that there are managers who are responsible for information security but are not experts in the field, especially in small- and medium-sized enterprises. The proposed model of P2 and P5 help them to gain an overview of the necessary areas to look at for the information security of an organization. Not only for non-experts but also for experts, the proposed model, as well as the dashboard, can help to illustrate the needs and shortcomings of the actual information security status of an organization to a higher level of management (board-members or business managers) and argue about necessary actions, the impact of these actions, and the value to the business. There is empirical evidence that the proposed solutions are easy to understand, simple ("in a good way"), and feasible for practitioners. Experts out of the interview within P5 suggested that an information security culture and commitment within the whole organization is required in order to implement a broad approach for information security assessment. The proposed result of this thesis is suitable to provide the basis for such an understanding within organizations.

Guide for information security metrics and indicators

Past literature, standards, and best practices such as ISO/IEC 27004 (ISO/IEC, 2009) or NIST SP 800-55 (NIST, 2008) support information security departments with suggested metrics to measure and monitor information security aspects of an organization. The shortcomings of these suggestions are that they are not covering the whole information security requirements (NIST, 2008) and do often measure only the effectiveness of the implementation of processes rather than the actual information security status (Bayuk, 2013). The thesis results of P3 and P5 contribute to these documents by providing a comprehensive list of metrics that are linked to information security management objectives and thus are measuring the aspects of the information security status itself and not the process implementation effectiveness. The list can be used to provide metrics for different measurement purposes of organizations and suggest a link to the actual measurement questions and objectives. The thesis contributes to standards and best practices and helps to implement a continuous improvement of the information security situation of an organization based on the proposed metrics.

Aggregation of already existing metrics

One result of P5 shows that most large organizations already have metrics for assessing information security, but face the same problems with a lack of clarity, structure, and consistent real-time data in their reports (Boehm et al., 2018). Also, the organizations are not sure about the usefulness of the existing metrics to quantify their objectives. The method to aggregate information security metrics (P4) can be used in order to aggregate existing metrics to indicators and develop comprehensive, understandable, and traceable indicators. These indicators will be used as a basis for the generation of dashboards, standard reports, and comparison tools to support decision making from existing metrics and data.

Target picture for information security assessment

Experts of the semi-structured interview expect the conceptual information security assessment dashboard to be a target picture for organizations in order to gain full transparency over the information security status of the organization - “which is the perfect view that you, as security responsible, need on your company” (expert statement). Therefore, P5 can be used as a target picture to implement an information security assessment program. The results of P2 and P5 answer practical questions of what data is necessary to measure aspects of information security or what areas of interest need to be addressed regarding information security. P5 also serves as an evaluation instrument that indicates whether an organization addresses all necessary aspects or not. For example, if an organization is not able to instantiate a metric with available data, it might be that this area has to be implemented in the future to comprehensively assess the information security status of this organization.

Decision support system on different management levels

By definition, a dashboard serves as a data-driven decision support system (Yigitbasioglu/Velcu, 2012). Therefore, the conceptual dashboard contributes to practice by providing a comprehensive decision support system for organizations in order to manage information security. The solution of P5 allows the comparison of key indicators and metrics between different organizations, organization departments, and locations because all of the metrics are connected to a base set of objects. To derive actions out of the current information security status, the solution provides a full trace-back to the root cause of the problem or weakness. For example, if a manager receives the indicator “number of vulnerabilities” that is too high, the manager has to know the root cause of this number. Various questions have to be answered to derive actions and reduce this number. For example, the questions: Which systems are affected? Are the affected systems important or critical for the business? Is the risk level high, medium, or small? What can a manager do to reduce or optimize this metric? P5 answers all these questions out of the proposed solution and allows a manager to trace down the aggregation to the root cause of the reported indicator or metric. In this way, possible actions can be derived directly from the dashboard. Because the aggregation methodology forms a tree-structure, each level of management or even functional departments can be served with the metrics and indicators they need. With this possibility, managers are able to measure, monitor, control, and identify the information security status relevant for them without looking at the whole dashboard and thus are confronted with negative effects on their decisions such as information overload.

Use as a common benchmark

P5 suggests that the conceptual information security assessment dashboard is not only feasible for the assessment of an organizations’ security but also to deliver the key indicators to others for benchmarking reasons. For example, the decision to select a cloud service provider is also dependent on the quality of service attribute security (Lang/Wiesche/Krcmar, 2018). Today, an indicator is the location of the servers because different countries have different stringent requirements in terms of information security and data protection. The P5 solution would also be useful for potential customers of the organizations to convince them of the quality of their information security. One concern that was indicated by experts in P5 is that this information is restricted and that even the indicators on the highest abstraction level tell too much about the actual information security status of an organization in the way, that these numbers are categorized as confidential and would not be made publicly available by any organization.

11 Study Limitations

The decisions made by choosing data gathering process, data analysis, and method selection cause limitations that have to be considered when interpreting the suggested results of this thesis. Limitations apply to all research. Therefore, various techniques are applied trying to minimize potential issues of validity and reliability.

The first limitation is based on the data gathering process. The data of P1, P2, and P3 are based on a literature search according to Webster/Watson (2002). The process of searching relevant articles includes the selection of databases and a restriction based on keywords. It can be argued, that important articles are missing based on the chosen selection that could have a major influence on the results. To minimize this issue, the articles were reviewed by the co-authors as well as discussed with experts in scientific conferences. This was also recommended by Webster/Watson (2002) which said that missing articles are "likely to be identified by colleagues who read your paper either prior to or after your submission". Additionally, P2 was evaluated with empirical data from a semi-structured expert interview. The other data - used in P2, P4, and P5 - are collected from semi-structured expert interviews and a focus group. The participants come from a limited number of organizations and industry sectors and thus are limited in generalizability. Also, the data of these interviews are subject to the interviewee's subjectivity and researcher's individual judgment (Mayring, 2015). To increase validity and reliability and therefore generalizability, several methods are applied. The results of P2, P4, and P5 are based on different data sources to provide richer empirical evidence. The research approach of this thesis includes three iterations to generate the results that are based upon each other. Each iteration was empirically validated with an overlapping but not equal expert group.

The data analysis process is subject to internal validity concerns. The data analysis was done by the author of the thesis and therefore might be subjectively biased. To reduce internal validity threats, the data analysis of P2, P4, and P5 are evaluated with additional empirical methods. P3 was validated within P4 and P5. Only P1 was not validated with additional methods and data. To increase validity and reliability, the available data - from literature and interviews - was analyzed based on standardized methods such as open-axial-selective coding or qualitative content analysis to increase validity and reliability. Also, different techniques were used to increase reliability based on (Mayring, 2015): (1) A part of the material was coded by different persons (the co-author) and tested if there are significantly high inconsistencies (also increases objectivity). (2) It was tested whether discrepancies in certain categories are common and solved by redefine them. (3) The reliability was increased by summarizing categories that are ambiguously different.

Design science is used to develop a conceptual information security assessment dashboard. According to Yigitbasioglu/Velcu (2012), dashboards are evaluated by their design features and the way the users interact with them to make decisions. Within this thesis, the dashboard is evaluated with a simulation study, a semi-structured expert interview and a focus group which are valid methods to evaluate a design science artifact (Hevner et al., 2004; Sonnenberg/Vom Brocke, 2012). The artifact was not implemented in practice and was thus examined for its applicability. Empirical evidence is given that an implementation of the proposed result is possible and the approach is feasible. There were some concerns articulated by the experts regarding the cost-effectiveness of gathering the necessary data to instantiate the conceptual dashboard while others mentioned that they could already fill the concept with the data available. A practical experiment using the conceptual dashboard in practice and evaluate the way the users interact with it was not done within this thesis.

There is a limitation based on the scope of the thesis in general. The phenomenon was examined from an organization's perspective on internal information security. Therefore, data was not included from sources that deal with outsourced information security functions and services. The results of this thesis support empirical evidence that the solution is also applicable to external organizations but it is questioned (by experts in practice) if these service providers would share the data of the dashboard to their customers. The view of an organization to the information security evaluation of external partners or entities could influence the proposed models and results based on a change of the perspective.

A limitation from a practical perspective could be, that the result is not tested if it complies with standards such as the ISO/IEC 27000. However, these standards are part of the original data and the results derive out of them, it can be assumed that the results are in line with the standards. Nevertheless, an empirical test of compliance is not provided.

12 Recommendations for Future Research

The findings of this thesis as well as the limitations outlined in the previous chapter provide various areas for future research. Especially a complex topic like information security needs a focus area of interest in order to contribute to a whole research stream. Therefore, various possible research questions arise by answering the research questions of this thesis.

Extending the model of information security factors for decision-makers

P2 introduces a comprehensive model of information security factors that influence information security managers' decisions. This model clusters several indicators and builds interdependencies between these clusters. These relationships can be studied with quantitative methods to further evaluate and extend the model. A possible way to improve generalizability would be a study that includes small- and medium-sized enterprises because the original data was mostly derived from interview experts within large organizations. Additionally, interdependencies between factors within the clusters can be explored. An example question could be: Is the reduction of vulnerabilities related to an improvement of the infrastructure weakness? These relationships on deeper levels of the model could be useful in order to improve the understanding of the whole security situation as well as to prioritize countermeasures according to them. Each individual factor of the model is a possibility to search for other influence factors other than security. An example would be that business continuity is an objective of improving information security and should be increased while simultaneously enhancing information security, but there may be other influencing factors that could be more important than information security. These factors were out of scope (information security) of this thesis.

Technical tools based on the conceptual results

Design science research is about the development of products, processes, constructs, design principles, models, methods, technological rules, and instantiations (Gregor/Hevner, 2013). Based on the results of P5, several tools can be further developed and multiple studies are possible. There is still a gap in tools to gather information security-related data and monitor the security status of an organization automatically (Wang/Wulf, 1997; Boyer/McQueen, 2007; Crossler et al., 2013). Experts in practice suggested the use of the information security assessment dashboard as a conceptual basis to develop tools for an automated collection of the necessary data. This would also serve as a solution for the experts' concerns regarding cost-effectiveness in gathering the necessary data to instantiate the dashboard. To develop these kinds of tools, possible areas of research would include the architecture, effectiveness, and usability of the tools as well as the possibility to collect the data automatically. The results of P2, P3, and P5 would serve as requirements for data gathering tools. The gathering of this information would open more possibilities such as the possibilities for automated recommender systems and active decision support systems for information security managers.

Studies based on the conceptual information security assessment dashboard

Future research could implement the dashboard in practice and evaluate it from the perspective of how managers interact with the dashboard in order to make decisions with them. From such studies, the decision-making process can be observed and possible rules or recommendations for practice as well as the understanding of the decision-making process in research can be extended and explored. Not only the dashboard can be evaluated in practice but also existing standards and best practices. Because the dashboard is an instance to measure the information security status of an organization, different countermeasures can be tested based on a possible improvement of the metrics and indicators. Empirical tests and rigorous studies of standards and best practices, which concern not only the effectiveness of the implementation of countermeasures but also the effectiveness of improving the level of information security, could be based on the suggested metrics and indicators and constitute an open research question in the literature (Siponen/Willison, 2009). P5 is also feasible to become a common standard for information security assessment or extension of existing ones. Another area for future research would be to compare the actual metrics and indicators between different organizations, industries, or departments in order to explore information security best practices.

Conceptual extension of the dashboard

Experts in practice recommended the extension of the dashboard to include financial implications to the organization as well as the costs to mitigate the risks based on the action alternatives that are served by the dashboard tree-structure (see results of P5). This would enable the business risk management to use the dashboard directly integrated into their processes.

Quantification of other phenomenons

P4 introduces a method to aggregate information security metrics based on different preconditions. The method can be pessimistic in the way of what you have not tested is vulnerable, results are comparable, traceable, actionable, understandable, comprehensive, and useful. These positive features could also be useful for other areas that have to be measured and aggregated to higher levels of management or to customers. An example would be to measure the complex phenomenon of cloud providers' trust (Lang/Wiesche/Krcmar, 2018), aggregate the metrics, and serve them to customers to prove their trustfulness such as other service level agreement parameters.

References

Abu-Musa, A. (2010): Information security governance in Saudi organizations: An empirical study. *Information Management & Computer Security*, Vol. 18, No. 4, pp. 226–276.

Afzal, W.; **Roland, D.**; **Al-Squri, M. N. (2009):** Information asymmetry and product valuation: an exploratory study. *Journal of Information Science*, Vol. 35, No. 2, pp. 192–203.

Ahmad, R.; **Sahib, S.**; **Azuwa, M. P. (2014):** Effective measurement requirements for network security management. *International Journal of Computer Science and Information Security*, Vol. 12, No. 4, pp. 1–8.

AIS Members (2011): Senior scholars' basket of journals. `https://aisnet.org/page/SeniorScholarBasket`, Last accessed 2020-03-02.

Akerlof, G. A. (1970): The Market for "Lemons": Quality Uncertainty and the Market Mechanism. *The Quarterly Journal of Economics*, Vol. 84, No. 3, pp. 488–500.

Al-Darwish, A. I.; **Choe, P. (2019):** A framework of information security integrated with human factors. *In HCI for Cybersecurity, Privacy and Trust*, Cham, Germany, Springer International Publishing, Lecture Notes in Computer Science, pp. 217–229.

Alavi, R.; **Islam, S.**; **Mouratidis, H. (2016):** An information security risk-driven investment model for analysing human factors. *Information and Computer Security*, Vol. 24, No. 2, pp. 205–227.

AlHogail, A. (2015): Design and validation of information security culture framework. *Computers in Human Behavior*, Vol. 49, pp. 567–575.

Almasizadeh, J.; **Azgomi, M. A. (2013):** A stochastic model of attack process for the evaluation of security metrics. *Computer Networks*, Vol. 57, No. 10, pp. 2159–2180.

Alqahtani, A. (2015): Towards a framework for the potential cyber-terrorist threat to critical national infrastructure. *Information and Computer Security*, Vol. 23, No. 5, pp. 532–569.

Alshaikh, M.; **Ahmad, A.**; **Maynard, S. B.**; **Chang, S. (2014):** Towards a taxonomy of information security management practices in organisations. *In 25th Australasian Conference on Information Systems*, Auckland, New Zealand, pp. 1–10.

Anderson, R.; **Moore, T. (2006):** The economics of information security. *Science (New York, N.Y.)*, Vol. 314, pp. 610–613.

Andress, J.; **Leary, M. (2017):** Building a practical information security program. Elsevier Inc.

Arabsorkhi, A.; **Ghaffari, F. (2018):** Security metrics: Principles and security assessment methods. *In 9th International Symposium on Telecommunication*, Tehran, Iran, IEEE, pp. 305–310.

Arora, A.; **Krishnan, R.**; **Telang, R.**; **Yang, Y. (2010):** An empirical analysis of software vendors' patch release behavior: Impact of vulnerability disclosure. *Information Systems Research*, Vol. 21, No. 1, pp. 115–132.

Ashenden, D. (2008): Information security management: A human challenge? *Information Security Technical Report*, Vol. 13, No. 4, pp. 195–201.

Atoum, I.; **Otoom, A.**; **Abu Ali, A. (2014):** A holistic cyber security implementation framework. *Information Management & Computer Security*, Vol. 22, No. 3, pp. 251–264.

Australian Cyber Security Growth Network Ltd. (2019): Australia's cyber security sector competitiveness plan 2019 update. Australian Cyber Security Growth Network Ltd., Technical Report.

Azuwa, M. P.; **Sahib, S.**; **Shamsuddin, S. (2017):** Technical security metrics model in compliance with ISO/IEC 27001 standard. *International Journal of Cyber–Security and Digital Forensics (IJCSDF)*, Vol. 1, No. 4, pp. 280–288.

Barki, H.; **Rivard, S.**; **Talbot, J. (1993):** Toward an Assessment of Software Development Risk. *Journal of Management Information Systems*, Vol. 10, No. 2, 203–225, ISSN 0742–1222.

Basili, R. V.; **Caldiera, G.**; **Rombach, H. D. (1994):** The goal question metric approach. *Encyclopedia of software engineering*,, pp. 528–532.

Basili, V. R.; **Weiss, D. M. (1984):** A methodology for collecting valid software engineering data. *IEEE Transactions on Software Engineering*, Vol. SE-10, No. 6, pp. 728–738.

Bayuk, J.; **Mostashari, A. (2013):** Measuring systems security. *Systems Engineering*, Vol. 16, No. 1, pp. 1–14.

Bayuk, J. L. (2011): Alternative security metrics. *In 2011 Eighth International Conference on Information Technology: New Generations*, Las Vegas, NV, USA, IEEE, pp. 943–946.

Bayuk, J. L. (2013): Security as a theoretical attribute construct. *Computers & Security*, Vol. 37, pp. 155–175.

Ben-Aissa, A.; **Abercrombie, R. K.**; **Sheldon, F. T.**; **Mili, A. (2012):** Defining and computing a value based cyber-security measure. *Information Systems and e-Business Management*, Vol. 10, No. 4, pp. 433–453.

Bentkower, M. (2017): Assessing the real damage of the 'WannaCry' malware attack. `https://www.commvault.com/blogs/2017/may/assessing-the-real-damage-of-the-wannacry-malware-attack`, Last accessed 2020-02-24.

Berander, P.; **Jönsson, P. (2006):** A goal question metric based approach for efficient measurement framework definition. *In ACM/IEEE International Symposium on Empirical Software Engineering*, New York, NY, USA, pp. 316–325.

Beresnevichiene, Y.; **Pym, D.**; **Shiu, S. (2010):** Decision support for systems security investment. *In IEEE/IFIP Network Operations and Management Symposium workshops*, Osaka, Japan, pp. 118–125.

Bernard, T. S.; **Cowley, S. (2017):** Equifax breach caused by lone employee's error, former C.E.O. says. `https://www.nytimes.com/2017/10/03/business/equifax-congress-data-breach.html`, Last accessed 2020-02-27.

Björck, F.; **Henkel, M.**; **Stirna, J.**; **Zdravkovic, J. (2015):** Cyber resilience - Fundamentals for a definition. *In New Contributions in Information Systems and Technologies*, Cham, Springer International Publishing, Advances in Intelligent Systems and Computing, pp. 311–316.

Black, P. E.; **Scarfone, K.**; **Souppaya, M. (2008):** Cyber security metrics and measures. *In Wiley Handbook of Science and Technology for Homeland Security*, Hoboken, NJ, USA, John Wiley & Sons Inc.

Bodin, L. D.; **Gordon, L. A.**; **Loeb, M. P. (2008):** Information security and risk management. *Communications of the ACM*, Vol. 51, No. 4, pp. 64–68.

Boehm, B. W. (1988): A spiral model of software development and enhancement. *Computer*, Vol. 21, No. 5, pp. 61–72.

Boehm, B. W. (1991): Software risk management: principles and practices. *IEEE Software*, Vol. 8, No. 1, pp. 32–41.

Boehm, J.; **Merrath, P.**; **Poppensieker, T.**; **Riemenschnitter, R.**; **Stähle, T. (2018):** Cyber risk measurement and the holistic cybersecurity approach. `https://www.mckinsey.com/business-functions/risk/our-insights/cyber-risk-measurement-and-the-holistic-cybersecurity-approach`, Last accessed 2020-02-28.

Bogner, A.; **Littig, B.**; **Menz, W. (2014):** Interviews mit experten: Eine praxisorientierte einführung. Springer Fachmedien Wiesbaden, Qualitative Sozialforschung.

Bogner, A.; **Menz, W. (2009):** The theory-generating expert interview: Epistemological interest, forms of knowledge, interaction. *In* **Bogner, A.**; **Littig, B.**; **Menz, W. eds.:** *Interviewing experts*, Basingstoke, Palgrave Macmillan, Research methods series, pp. 43–80.

Böhme, R. (2010): Security metrics and security investment models. *In Advances in Information and Computer Security*, Berlin, Heidelberg, Springer Berlin Heidelberg, pp. 10–24.

Bojanc, R.; **Jerman-Blažič, B. (2008):** An economic modelling approach to information security risk management. *International Journal of Information Management*, Vol. 28, No. 5, pp. 413–422.

Bortz, J.; **Döring, N. (1995):** Forschungsmethoden und evaluation. Springer-Verlag Berlin Heidelberg, Springer-Lehrbuch.

Boss, S. R.; **Kirsch, L. J.**; **Angermeier, I.**; **Shingler, R. A.**; **Boss, R. W. (2009):** If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems*, Vol. 18, No. 2, pp. 151–164.

Boyer, W.; **McQueen, M. (2007):** Ideal based cyber security technical metrics for control systems. *In Critical information infrastructures security*, Malaga, Spain, pp. 246–260.

Boyer, W. F.; **McQueen, M. A. (2008):** Primer control system cyber security framework and technical metrics. (INL/EXT-08-14324) Technical Report.

Brotby, W. K. (2009): Information security management metrics: A definitive guide to effective security monitoring and measurement. Boca Raton, FL, Florida, CRC Press, ebrary, Inc.

Bundesanzeiger (2015): Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz). *Bundesgesetzblatt*, Vol. 1, No. 31, pp. 1324–1331.

Butcher, H. (1995): Information overload in management and business. *In IEE Colloquium on Information Overload*, London, UK, pp. 1/1–1/2.

Cavusoglu, H.; **Mishra, B.**; **Raghunathan, S. (2004):** A model for evaluating IT security investments. *Communications of the ACM*, Vol. 47, No. 7, pp. 87–92.

CCIB (2017): Common criteria for information technology security evaluation – Part 2: Security functional components, Version 3.1, Revision 5. Common Criteria.

Chai, S.; **Kim, M.**; **Rao, H. R. (2011):** Firms' information security investment decisions: Stock market evidence of investors' behavior. *Decision Support Systems*, Vol. 50, No. 4, pp. 651–661.

Chakraborty, A.; **Sengupta, A.**; **Mazumdar, C. (2012):** A formal approach to information security metrics. *In 3rd International Conference on Emerging Applications of Information Technology*, Kolkata, India, IEEE, pp. 439–442.

Cisco Systems Inc. (2018): Cisco 2018: Annual cybersecurity report. Cisco Systems Inc., Technical Report.

Clark, K.; **Dawkins, J.**; **Hate, J. (2005):** Security risk metrics: fusing enterprise objectives and vulnerabilities. *In 6th Annual IEEE Systems, Man and Cybernetics (SMC) Information Assurance Workshop*, West Point, NY, USA, IEEE, pp. 388–393.

Collier, Z. A.; **Panwar, M.**; **Ganin, A. A.**; **Kott, A.**; **Linkov, I. (2016):** Security metrics in industrial control systems. *In Cyber-security of SCADA and other industrial control systems*, Switzerland, Springer, Advances in Information Security, pp. 167–185.

Cooper, H. M. (1988): Organizing knowledge syntheses: A taxonomy of literature reviews. *Knowledge in Society*, Vol. 1, No. 1, pp. 104–126.

Corbin, J.; **Strauss, A. (1990):** Grounded theory research: Procedures, canons and evaluative criteria. *Qualitative Sociology*, Vol. 13, No. 1, pp. 3–21.

Coronado, A. S.; **Mahmood, M. A.**; **Pahnila, S.**; **Luciano, E. M. (2009):** Measuring effectiveness of information systems security: An empirical research. *In 15th Americas Conference on Information Systems*, San Francisco, California, pp. 2175–2182.

Crossler, R.; **Belanger, F. (2012):** The quest for complete security protection: An empirical analysis of an individual's 360 degree protection from file and data loss. *In 18th Americas Conference on Information Systems*, Seattle, Washington, USA.

Crossler, R. E.; **Johnston, A. C.**; **Lowry, P. B.**; **Hu, Q.**; **Warkentin, M.**; **Baskerville, R. (2013):** Future directions for behavioral information security research. *Computers & Security*, Vol. 32, pp. 90–101.

Csaszar, F. A.; **Eggers, J. P. (2013):** Organizational decision making: An information aggregation view. *Management Science*, Vol. 59, No. 10, pp. 2257–2277.

Cyert, R. M.; **March, J. G. (1963):** A behavioral theory of the firm. *Englewood Cliffs*, Vol. 2, No. 4, pp. 169–187.

D'Arcy, J.; **Herath, T. (2011):** A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. *European Journal of Information Systems*, Vol. 20, No. 6, pp. 643–658.

DeLone, W. H.; **McLean, E. R. (1992):** Information systems success: The quest for the dependent variable. *Information Systems Research*, Vol. 3, No. 1, pp. 60–95.

Dhillon, G.; **Backhouse, J. (2001):** Current directions in IS security research: Towards socio-organizational perspectives. *Information Systems Journal*, Vol. 11, No. 2, pp. 127–153.

Dhillon, G.; **Torkzadeh, G. (2006):** Value-focused assessment of information system security in organizations. *Information Systems Journal*, Vol. 16, No. 3, pp. 293–314.

Diesch, R.; **Krcmar, H. (2020):** SoK: Linking information security metrics to management success factors. *In 15th International Conference on Availability, Reliability and Security (ARES 2020)*, Virtual Event, Ireland, pp. 1–10.

Diesch, R.; **Pfaff, M.**; **Krcmar, H. (2018):** Prerequisite to measure information security: A state of the art literature review. *In 4th International Conference on Information Systems Security and Privacy (ICISSP)*, Madeira, Portugal, pp. 207–215.

Diesch, R.; **Pfaff, M.**; **Krcmar, H. (2020):** A comprehensive model of information security factors for decision-makers. *Computers & Security*, Vol. 92, pp. 1–21.

Dinev, T.; **Goo, J.**; **Hu, Q.**; **Nam, K. (2009):** User behaviour towards protective information technologies: The role of national cultural differences. *Information Systems Journal*, Vol. 19, No. 4, pp. 391–412.

Dinev, T.; **Hu, Q. (2007):** The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems*, Vol. 8, No. 7, pp. 386–408.

Dogaheh, M. A. (2010): Introducing a framework for security measurements. *In IEEE International Conference on Information Theory and Information Security*, Beijing, China, pp. 638–641.

Doherty, N. F.; **Anastasakis, L.**; **Fulford, H. (2009):** The information security policy unpacked: A critical study of the content of university policies. *International Journal of Information Management*, Vol. 29, No. 6, pp. 449–457.

Doynikova, E.; **Fedorchenko, A.**; **Kotenko, I. (2019):** Ontology of Metrics for Cyber Security Assessment. *In 14th International Conference on Availability, Reliability and Security*, New York, NY, USA, ACM Press, pp. 1–8.

Driver, M. J.; **Mock, T. J. (1975):** Human information processing, decision style theory, and accounting information systems. *The Accounting Review*, Vol. 50, No. 3, pp. 490–508.

Drugescu, C.; **Etges, R. (2006):** Maximizing the return on investment on information security programs: Program governance and metrics. *Information Systems Security*, Vol. 15, No. 6, pp. 30–40.

Dzazali, S.; **Sulaiman, A.**; **Zolait, A. H. (2009):** Information security landscape and maturity level: Case study of Malaysian Public Service (MPS) organizations. *Government Information Quarterly*, Vol. 26, No. 4, pp. 584–593.

Eckert, C. (2013): IT-Sicherheit: Konzepte - Verfahren - Protokolle. 8. Edition. Oldenbourg Wissenschaftsverlag GmbH.

edgescan (2018): 2018 Vulnerability statistics report. BCC Risk Advisory Ltd., Technical Report.

Enterprise Management Associates, Inc (2017): A day in the life of a cyber security pro. Enterprise Management Associates, Inc, Technical Report.

Ernest Chang, S.; **Ho, C. B. (2006):** Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems*, Vol. 106, No. 3, pp. 345–361.

Etner, J.; **Jeleva, M.**; **Tallon, J.-M. (2012):** Decision theory under ambiguity. *Journal of Economic Surveys*, Vol. 26, No. 2, pp. 234–270.

Feng, N.; **Li, M. (2011):** An information systems security risk assessment model under uncertain environment. *Applied Soft Computing*, Vol. 11, No. 7, pp. 4332–4340.

Fenz, S.; **Heurix, J.**; **Neubauer, T.**; **Pechstein, F. (2014):** Current challenges in information security risk management. *Information Management & Computer Security*, Vol. 22, No. 5, pp. 410–430.

Fenz, S.; **Neubauer, T.**; **Accorsi, R.**; **Koslowski, T. (2013):** FORISK: Formalizing information security risk and compliance management. *In 43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop*, Budapest, Hungary, pp. 1–4.

Flexera (2018): Vulnerability review 2018 - Global trends - Key figures and facts on vulnerabilities from a global information security perspective. Flexera, Executive Report.

Freund, J. (2015): Measuring and managing information risk: A FAIR approach. Amsterdam, Elsevier Inc.

Frizell, S. (2015): Sony the interview hack: studio spending $15 million to deal with it. `http://time.com/3695118/sony-hack-the-interview-costs`, Last accessed 2020-02-24.

Gao, X.; **Zhong, W. (2015):** Information security investment for competitive firms with hacker behavior and security requirements. *Annals of Operations Research*, Vol. 235, No. 1, pp. 277–300.

Gartner Inc. (2017): Make the best of shadow IT. `https://www.gartner.com/smarterwithgartner/make-the-best-of-shadow-it/`, Last accessed 2020-03-04.

Geer, D.; **Hoo, K. S.**; **Jaquith, A. (2003):** Information security: Why the future belongs to the quants. *IEEE Security & Privacy Magazine*, Vol. 1, No. 4, pp. 24–32.

Glaser, B. G.; **Strauss, A. L. (1967):** The discovery of grounded theory: Strategies for qualitative research. New Brunswick, USA, Aldine Transaction.

Goel, S.; **Chengalur-Smith, I. N. (2010):** Metrics for characterizing the form of security policies. *The Journal of Strategic Information Systems*, Vol. 19, No. 4, pp. 281–295.

Goldstein, J.; **Chernobai, A.**; **Benaroch, M. (2011):** An event study analysis of the economic impact of IT operational risk and its subcategories. *Journal of the Association for Information Systems*, Vol. 11, No. 9, pp. 606–631.

Gonzalez, J. J.; **Sawicka, A. (2002):** A framework for human factors in information security. *In International Conference on Information Security, Hardware/Software Codesign, E-Commerce and Computer Networks (WSEAS)*, Rio de Janeiro, Brazil, pp. 1871–1877.

Gosavi, H. R.; **Bagade, A. M. (2015):** A review on zero day attack safety using different scenarios. *European Journal of Advances in Engineering and Technology*, Vol. 2, No. 1, pp. 30–34.

Grant, K.; **Edgar, D.**; **Sukumar, A.**; **Meyer, M. (2014):** 'Risky business': Perceptions of e-business risk by UK small and medium sized enterprises (SMEs). *International Journal of Information Management*, Vol. 34, No. 2, pp. 99–122.

Gregor, S.; **Hevner, A. R. (2013):** Positioning and presenting design science research for maximum impact. *MIS Quarterly*, Vol. 37, No. 2, pp. 337–355.

Gritzalis, D.; **Iseppi, G.**; **Mylonas, A.**; **Stavrou, V. (2018):** Exiting the risk assessment maze: A meta-survey. *ACM Computing Surveys*, Vol. 51, No. 1, pp. 1–30.

Gupta, A.; **Hammond, R. (2005):** Information systems security issues and decisions for small businesses. *Information Management & Computer Security*, Vol. 13, No. 4, pp. 297–310.

Güver, S.; **Motschnig, R. (2017):** Expert evaluation of commct, a communication model for multicultural teams. *Journal of Interaction Science (JoIS)*, Vol. 5, No. 1, pp. 1–19.

Hajdarevic, K.; **Allen, P. (2013):** A new method for the identification of proactive information security management system metrics. *In 36th International Convention on Information & Communication Technology, Electronics & Microelectronics (MIRPO)*, Opatija, Croatia, pp. 1121–1126.

Hajdarevic, K.; **Pattinson, C.**; **Kozaric, K.**; **Hadzic, A. (2012):** Information security measurement infrastructure for KPI visualization. *In 35th International Convention on Information & Communication Technology, Electronics & Microelectronics (MIRPO)*, Opatija, Croatia, pp. 1543–1548.

Hall, J. H.; **Sarkani, S.**; **Mazzuchi, T. A. (2011):** Impacts of organizational capabilities in information security. *Information Management & Computer Security*, Vol. 19, No. 3, pp. 155–176.

Haqaf, H.; **Koyuncu, M. (2018):** Understanding key skills for information security managers. *International Journal of Information Management*, Vol. 43, pp. 165–172.

Hayden, L. (2010): IT security metrics: A practical framework for measuring security & protecting data. New York, McGraw Hill.

Hedström, K.; **Kolkowska, E.**; **Karlsson, F.**; **Allen, J. P. (2011):** Value conflicts for information security management. *The Journal of Strategic Information Systems*, Vol. 20, No. 4, pp. 373–384.

Herath, T.; **Chen, R.**; **Wang, J.**; **Banjara, K.**; **Wilbur, J.**; **Rao, H. R. (2014):** Security services as coping mechanisms: An investigation into user intention to adopt an email authentication service. *Information Systems Journal*, Vol. 24, No. 1, pp. 61–84.

Herath, T.; **Rao, H. R. (2009):** Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, Vol. 18, No. 2, pp. 106–125.

Herrera, S. (2005): Information security management metrics development. *In 39th Annual 2005 International Carnahan Conference on Security Technology*, Las Palmas, Spain, pp. 51–56.

Herrmann, D. S. (2007): Complete guide to security and privacy metrics: Measuring regulatory compliance, operational resilience, and ROI. Boston, MA, USA, Auerbach Publications.

Herzog, A.; **Shahmehri, N.**; **Duma, C. (2007):** An ontology of information security. *International Journal of Information Security and Privacy*, Vol. 1, No. 4, pp. 1–23.

Hevner, A. R.; **March, S. T.**; **Park, J.**; **Ram, S. (2004):** Design science in information systems research. *MIS Quarterly*, Vol. 28, No. 1, pp. 75–105.

Holm, H.; **Afridi, K. K. (2015):** An expert-based investigation of the common vulnerability scoring system. *Computers & Security*, Vol. 53, pp. 18–30.

Höne, K.; **Eloff, J. (2002):** Information security policy – what do international information security standards say? *Computers & Security*, Vol. 21, No. 5, pp. 402–409.

Hong, K.-S.; **Chi, Y.-P.**; **Chao, L. R.**; **Tang, J.-H. (2003):** An integrated system theory of information security management. *Information Management & Computer Security*, Vol. 11, No. 5, pp. 243–248.

Horne, C. A.; **Maynard, S. B.**; **Ahmad, A. (2017):** Information security strategy in organisations: Review, discussion and future research. *Australasian Journal of Information Systems*, Vol. 21, pp. 1–17.

Hu, Q.; **Dinev, T.**; **Hart, P.**; **Cooke, D. (2012):** Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, Vol. 43, No. 4, pp. 615–660.

Hua, J.; **Bapna, S. (2013):** The economic impact of cyber terrorism. *The Journal of Strategic Information Systems*, Vol. 22, No. 2, pp. 175–186.

Hwang, M. I.; **Lin, J. W. (1999):** Information dimension, information overload and decision quality. *Journal of Information Science*, Vol. 25, No. 3, pp. 213–218.

IBM Institute for Business Value (2018): Cybersecurity in the cognitive era - Priming your digital immune system. IBM Corporation, Executive Report.

(ICS)^2 (2018): Cybersecurity professionals focus on developing new skills as workforce gap widens - (ISC)^2 cybersecurity workforce study. (ICS)^2, Technical Report.

Idika, N.; **Bhargava, B. (2012):** Extending attack graph-based security metrics and aggregating their application. *IEEE Transactions on Dependable and Secure Computing*, Vol. 9, No. 1, pp. 75–85.

Ifinedo, P. (2012): Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, Vol. 31, No. 1, pp. 83–95.

ISACA (2012): COBIT 5: A business framework for the governance and management of enterprise IT. Information Systems Audit and Control Association.

ISF (2018): Standard of good practice for information security. Information Security Forum Limited (ISF), Technical Report.

ISO/IEC (2005): ISO/IEC 27001:2005(E) - Information technology - Security techniques - Information security management systems - Requirements. Switzerland, ISO/IEC, Standard.

ISO/IEC (2009): ISO/IEC 27004:2009(E): Information technology - Security techniques - Information security management - Measurement. Switzerland, ISO/IEC, Technical Report.

ISO/IEC (2018): ISO/IEC 27000:2018(E): Information technology - Security techniques - Information security management systems - Overview and vocabulary. Switzerland, ISO/IEC, Standard.

IT Governance Institute (2007): COBIT 4.1: Framework, control objectives, management guidelines, maturity models. Rolling Meadows, IT Governance Institute.

Jafari, S.; **Mtenzi, F.**; **Fitzpatrick, R.**; **O'Shea, B. (2010):** Security metrics for e-healthcare information systems: A domain specific metrics approach. *International Journal of Digital Society (IJDS)*, Vol. 1, No. 4, pp. 238–245.

Jean Camp, L.; **Wolfram, C. (2004):** Pricing security: Vulnerabilities as externalities. *Economics of Information Security*, Vol. 12, pp. 17–34.

Jha, S.; **Sheyner, O.**; **Wing, J. (2002):** Two formal analys s of attack graphs. *In 15th IEEE Computer Security Foundations Workshop*, Cape Breton, NS, Canada, pp. 49–63.

Joh, H.; **Malaiya, Y. K. (2011):** Defining and assessing quantitative security risk measures using vulnerability lifecycle and CVSS metrics. *In International Conference on Security and Management*, Las Vegas, Nevada, USA, pp. 10–16.

Johannesson, P.; **Perjons, E. (2014):** An introduction to design science. Cham, Springer International Publishing.

Johnson, M. E.; **Goetz, E. (2007):** Embedding information security into the organization. *IEEE Security & Privacy Magazine*, Vol. 5, No. 3, pp. 16–24.

Johnston, A. C.; **Warkentin, M.**; **McBride, M.**; **Carter, L. (2016):** Dispositional and situational factors: Influences on information security policy violations. *European Journal of Information Systems*, Vol. 25, No. 3, pp. 231–251.

Jones, R. A.; **Horowitz, B. (2012):** A system-aware cyber security architecture. *Systems Engineering*, Vol. 15, No. 2, pp. 225–240.

Jonsson, E.; **Pirzadeh, L. (2011):** A framework for security metrics based on operational system attributes. *In 3rd International Workshop on Security Measurements and Metrics*, Banff, AB, Canada, IEEE, pp. 58–65.

Kahn, D. (1967): Codebreakers. Macmillan Company.

Kahn, D. (1997): The codebreakers: The comprehensive history of secret communication from ancient times to the Internet. Rev. and updated ed. Edition. New York, Scribner's and Sons.

Kankanhalli, A.; **Teo, H.-H.**; **Tan, B. C.**; **Wei, K.-K. (2003):** An integrative study of information systems security effectiveness. *International Journal of Information Management*, Vol. 23, No. 2, pp. 139–154.

Karjalainen, M.; **Siponen, M. (2011):** Toward a new meta-theory for designing information systems (IS) security training approaches. *Journal of the Association for Information Systems*, Vol. 12, No. 8, pp. 518–555.

Katos, V.; **Adams, C. (2005):** Modelling corporate wireless security and privacy. *The Journal of Strategic Information Systems*, Vol. 14, No. 3, pp. 307–321.

Knapp, K.; **Marshall, T.**; **Rainer, R. K.**; **Morrow, D. (2006):** The top information security issues facing organizations: What can government do to help? *Information Systems Security*, Vol. 15, No. 4, pp. 51–58.

Knapp, K. J.; **Franklin Morris, R.**; **Marshall, T. E.**; **Byrd, T. A. (2009):** Information security policy: An organizational-level process model. *Computers & Security*, Vol. 28, No. 7, pp. 493–508.

Koontz, H. (1980): The management theory jungle revisited. *The Academy of Management Review*, Vol. 5, No. 2, pp. 175–187.

Kotenko, I.; **Bogdanov, V. (2009):** Proactive monitoring of security policy accomplishment in computer networks. *In 5th IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems, Technology and Applications*, Rende, Italy, pp. 364–369.

Kotenko, I.; **Doynikova, E. (2013):** Security metrics for risk assessment of distributed information systems. *In 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS)*, IEEE, pp. 646–650.

Kotulic, A. G.; **Clark, J. G. (2004):** Why there aren't more information security research studies. *Information & Management*, Vol. 41, No. 5, pp. 597–607.

Kovacich, G. (1997): Information systems security metrics management. *Computers & Security*, Vol. 16, No. 7, pp. 610–618.

Kraemer, S.; **Carayon, P.**; **Clem, J. (2009):** Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & Security*, Vol. 28, No. 7, pp. 509–520.

Krcmar, H. (2015): Einführung in das Informationsmanagement. 2. Edition. Berlin, Heidelberg, Springer Gabler, Springer-Lehrbuch.

Kumar, R. L.; **Park, S.**; **Subramaniam, C. (2008):** Understanding the value of countermeasure portfolios in information systems security. *Journal of Management Information Systems*, Vol. 25, No. 2, pp. 241–280.

Lang, M.; **Wiesche, M.**; **Krcmar, H. (2018):** Criteria for selecting cloud service providers: A delphi study of quality-of-service attributes. *Information & Management*, Vol. 55, No. 6, pp. 746–758.

Lee, C. H.; **Geng, X.**; **Raghunathan, S. (2016):** Mandatory standards and organizational information security. *Information Systems Research*, Vol. 27, No. 1, pp. 70–86.

Lee, Y.; **Larsen, K. R. (2009):** Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems*, Vol. 18, No. 2, pp. 177–187.

Leeuw, K. M. M. de; **Bergstra, J. A.**; **Bergstra, J.**; **Bergstra, J. A.**; **Leeuw, K. d.**; **Maria Michael de Leeuw, K. (2007):** History of information security: A comprehensive handbook. Elsevier Science B.V.

LeMay, E.; **Ford, M. D.**; **Keefe, K.**; **Sanders, W. H.**; **Muehrcke, C. (2011):** Model–based security metrics using adversary view security evaluation (ADVISE). *In Eighth International Conference on Quantitative Evaluation of SysTems*, Aachen, Germany, pp. 191–200.

Leon, P. G.; **Saxena, A. (2010):** An approach to quantitatively measure information security. *In 3rd India Software Engineering Conference*, Mysore, India.

Levy, Y.; **J. Ellis, T. (2006):** A systems approach to conduct an effective literature review in support of information systems research. *Informing Science: The International Journal of an Emerging Transdiscipline*, Vol. 9, pp. 181–212.

Liang, H.; **Xue, Y. (2009):** Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly*, Vol. 33, No. 1, pp. 71–90.

Lowry, P. B.; **Moody, G. D. (2015):** Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. *Information Systems Journal*, Vol. 25, No. 5, pp. 433–463.

Maier, J.; **Padmos, A.**; **S. Bargh, M.**; **Wörndl, W. (2017):** Influence of mental models on the design of cyber security dashboards. *In 12th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications*, Porto, Portugal, SCITEPRESS - Science and Technology Publications, pp. 128–139.

Malekovic, N.; **Sutanto, J.**; **Goutas, L. (2016):** Manipulative imputation in distributed decision support settings: The implications of information asymmetry and aggregation complexity. *Decision Support Systems*, Vol. 85, pp. 1–11.

Manhart, M.; **Thalmann, S. (2015):** Protecting organizational knowledge: A structured literature review. *Journal of Knowledge Management*, Vol. 19, No. 2, pp 190–211.

March, S. T.; **Smith, G. F. (1995):** Design and natural science research on information technology. *Decision Support Systems*, Vol. 15, No. 4, pp. 251–266, ISSN 01679236.

May, T. A. (1997): The death of ROI: re–thinking IT value measurement. *Information Management & Computer Security*, Vol. 5, No. 3, pp. 90–92.

Mayring, P. (2015): Qualitative inhaltsanalyse: Grundlagen und techniken. Weinheim, Germany, Beltz, Beltz Pädagogik.

Mazur, K.; **Ksiezopolski, B.**; **Kotulski, Z. (2015):** The robust measurement method for security metrics generation. *The Computer Journal*, Vol. 58, No. 10, pp. 2280–2296.

McKenna, S.; **Staheli, D.**; **Fulcher, C.**; **Meyer, M. (2016):** BubbleNet: A cyber security dashboard for visualizing patterns. *Computer Graphics Forum*, Vol. 35, No. 3, pp. 281–290.

Merete Hagen, J.; **Albrechtsen, E.**; **Hovden, J. (2008):** Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security*, Vol. 16, No. 4, pp. 377–397.

Mermigas, D.; **Patsakis, C.**; **Pirounias, S. (2013):** Quantification of information systems security with stochastic calculus. *In 8th Annual Cyber Security and Information Intelligence Research Workshop*, Oak Ridge, Tennessee, USA, pp. 1–9.

Meuser, M.; **Nagel, U. (2009):** The expert interview and changes in knowledge production. *In* **Bogner, A.**; **Littig, B.**; **Menz, W. eds.:** *Interviewing experts*, Basingstoke, Palgrave Macmillan, Research methods series, pp. 17–42.

Mijnhardt, F.; **Baars, T.**; **Spruit, M. (2016):** Organizational characteristics influencing SME information security maturity. *Journal of Computer Information Systems*, Vol. 56, No. 2, 106–115.

Mishra, S.; **Chasalow, L. (2011):** Information security effectiveness: A research framework. *Issues in Information Systems*, Vol. 7, No. 1, pp. 246–255.

M'manga, A.; **Faily, S.**; **McAlaney, J.**; **Williams, C.**; **Kadobayashi, Y.**; **Miyamoto, D. (2019):** A normative decision-making model for cyber security. *Information & Computer Security*, Vol. 26, No. 5, pp. 636–646.

Montesdioca, G. P. Z.; **Maçada, A. C. G. (2015):** Measuring user satisfaction with information security practices. *Computers & Security*, Vol. 48, pp. 267–280.

Morgan, M. G.; **Henrion, M. (1992):** Uncertainty: A guide to dealing with uncertainty in quantitative risk and policy analysis. Cambridge, Cambridge Univ. Press.

Muthukrishnan, S. M.; **Palaniappan, S. (2016):** Security metrics maturity model for operational security. *In IEEE Symposium on Computer Applications and Industrial Electronics*, Penang, Malaysia, pp. 101–106.

Narain Singh, A.; **Gupta, M. P.**; **Ojha, A. (2014):** Identifying factors of "organizational information security management". *Journal of Enterprise Information Management*, Vol. 27, No. 5, pp. 644–667.

Nazareth, D. L.; **Choi, J. (2015):** A system dynamics model for information security management. *Information & Management*, Vol. 52, No. 1, pp. 123–134.

Neumann, J. von; **Morgenstern, O. (1944):** Theory of games and economic behavior. *Science and Society*, Vol. 9, No. 4, pp. 366–369.

Nichols, E. A.; **Sudbury, A. (2006):** Implementing security metrics initiatives. *EDPACS - The EDP Audit, Control, and Security Newsletter*, Vol. 34, No. 3, pp. 10–20.

NIST (2008): NIST SP 800-55r1: Performance measurement guide for information security. National Institute of Standards and Technology, NIST, S. P., Technical Report.

NIST (2013a): NIST SP 800-53r4: Security and privacy controls for federal information systems and organizations. National Institute of Standards and Technology, NIST, S. P., Technical Report.

NIST (2013b): NISTIR 7298r2: Glossary of key information security terms. National Institute of Standards and Technology, NIST, S. P., Technical Report.

NIST (2015): NIST SP 800-30r1: Risk management guide for information technology systems. National Institute of Standards and Technology, NIST, S. P., Technical Report.

NIST (2018a): NIST SP 800-37r2: Risk management framework for information systems and organizations. National Institute of Standards and Technology, NIST, S. P., Technical Report.

NIST (2018b): NIST special publication 800-series general information. `https://www.nist.gov/itl/nist-special-publication-800-series-general-information`, Last accessed 2020-02-27.

Norman, A. A.; **Yasin, N. M. (2012):** Information systems security management (ISSM) success factor: Retrospection from the scholars. *In 11th European Conference on Information warfare and security*, Laval, France, pp. 339–344.

Norman, A. A.; **Yasin, N. M. (2013):** Information systems security management (ISSM) success factor: Retrospection from the scholars. *African Journal of Business Management*, Vol. 7, No. 27, pp. 2646–2656.

Office of the Law Revision Counsel (2007): Title 38 - VETERANS' BENEFITS §5727. *United States Code*, Vol. 1, pp. 684–685.

Onibere, M.; **Ahmad, A.**; **Maynard, S. (2017):** The chief information security officer and the five dimensions of a strategist. *In Pacific Asia Conference on Information Systems (PACIS 2017)*, Langkawi Island, Malaysia, pp. 1–12.

Onwuegbuzie, A. J.; **Dickinson, W. B.**; **Leech, N. L.**; **Zoran, A. G. (2009):** A qualitative framework for collecting and analyzing data in focus group research. *International Journal of Qualitative Methods*, Vol. 8, No. 3, 1–21.

Osvaldo De Sordi, J.; **Meireles, M.**; **Carvalho de Azevedo, M. (2014):** Information selection by managers: Priorities and values attributed to the dimensions of information. *Online Information Review*, Vol. 38, No. 5, pp. 661–679.

Payne, J. W.; **Bettman, J. R.**; **Johnson, E. J. (1988):** Adaptive strategy selection in decision making. *Journal of Experimental Psychology: Learning, Memory, and Cognition*, Vol. 14, No. 3, pp. 534–552.

Peffers, K.; **Tuunanen, T.**; **Rothenberger, M.**; **Chatterjee, S. (2007):** A design science research methodology for information systems research. *Journal of Management Information Systems*, Vol. 24, No. 3, pp. 45–77.

Pendleton, M.; **Garcia-Lebron, R.**; **Cho, J.-H.**; **Xu, S. (2017):** A survey on systems security metrics. *ACM Computing Surveys*, Vol. 49, No. 4, pp. 1–35.

Phillips, C.; **Swiler, L. P. (1998):** A graph-based system for network-vulnerability analysis. *In Proceedings of the 1998 Workshop on New Security Paradigms*, Charlottesville, Virginia, USA, pp. 71–79.

Polasky, S.; **Carpenter, S. R.**; **Folke, C.**; **Keeler, B. (2011):** Decision-making under great uncertainty: Environmental management in an era of global change. *Trends in Ecology & Evolution*, Vol. 26, No. 8, pp. 398–404.

Ponemon Institute LLC (2018): 2018 Cost of a data breach study: Global overview. Ponemon Institute LLC, Technical Report.

Posey, C.; **Roberts, T. L.**; **Lowry, P. B. (2015):** The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems*, Vol. 32, No. 4, pp. 179–214.

Prat, N.; **Comyn-Wattiau, I.**; **Akoka, J. (2014):** Artifact evaluation in information systems design-science research: A holistic view. *In Pacific Asia Conference on Information Systems*, Chengdu, China.

Premaratne, U.; **Samarabandu, J.**; **Sidhu, T.**; **Beresh, B.**; **Tan, J.-C. (2008):** Application of security metrics in auditing computer network security: A case study. *In 4th International Conference on Information and Automation for Sustainability*, Colombo, Sri Lanka, pp. 200–205.

Pudar, S.; **Manimaran, G.**; **Liu, C.-C. (2009):** PENET: A practical method and tool for integrated modeling of security attacks and countermeasures. *Computers & Security*, Vol. 28, No. 8, pp. 754–771.

Purboyo, T. W.; **Rahardjo, B.**; **Kuspriyanto (2011):** Security metrics: A brief survey. *In 2nd International Conference on Instrumentation, Communications, Information Technology and Biomedical Engineering*, Bandung, Indonesia, pp. 79–82.

Qassim, Q. S.; **Jamil, N.**; **Daud, M.**; **Patel, A.**; **Ja'affar, N. (2019):** A review of security assessment methodologies in industrial control systems. *Information and Computer Security*, Vol. 27, No. 1, pp. 47–61.

Radianti, J.; **Gjøsæter, T. (2017):** Metrics for ensuring security and privacy of information sharing platforms for improved city resilience. *International Journal of Information Systems for Crisis Response and Management*, Vol. 9, No. 3, pp. 36–54.

Ransbotham, S.; **Mitra, S. (2009):** Choice and chance: A conceptual model of paths to information security compromise. *Information Systems Research*, Vol. 20, No. 1, pp. 121–139.

Ravenel, J. P. (2006): Effective Operational Security Metrics. *Information Systems Security*, Vol. 15, No. 3, pp. 10–17.

Robinson, S. (2004): Simulation modelling: The practice of model developmenrand use. Chichester, John Wiley & Sons, Inc.

Rudolph, M.; **Schwarz, R. (2012):** A critical survey of security indicator approaches. *In 7th International Conference on Availability, Reliability and Security*, Prague, Czech Republic, pp. 291–300.

Ryan, J. J.; **Ryan, D. J. (2008):** Performance metrics for information security risk management. *IEEE Security & Privacy*, Vol. 6, No. 5, pp. 38–44.

Samonas, S.; **Dhillon, G.**; **Almusharraf, A. (2020):** Stakeholder perceptions of information security policy: Analyzing personal constructs. *International Journal of Information Management*, Vol. 50, pp. 144–154.

Savage, L. J. (1954): The foundations of statistics. New York, NY, USA, J. Wiley.

Savola, R. (2007): Towards a security metrics taxonomy for the information and communication technology industry. *In International Conference on Software Engineering Advances (ICSEA)*, Cap Esterel, France, pp. 60–66.

Savola, R. M. (2009): A security metrics taxonomization model for software-intensive systems. *Journal of Information Processing Systems*, Vol. 5, No. 4, pp. 197–206.

Savola, R. M. (2013): Quality of security metrics and measurements. *Computers & Security*, Vol. 37, pp. 78–90.

Savola, R. M.; **Heinonen, P. (2011):** A visualization and modeling tool for security metrics and measurements management. *In 2011 Information Security for South Africa*, Johannesburg, South Africa, pp. 1–8.

Schneier, B. (2003): Beyond fear: Thinking sensibly about security in an uncertain world. 1. Edition. New York, Springer Science and Business Media.

Sharman, R.; **Rao, R.**; **Upadhyaya, S. (2004):** Metrics for information security: A literature review. *In 10th Americas Conference on Information Systems*, New York, NY, USA, pp. 1437–1440.

Silic, M.; **Back, A. (2014):** Information security: Critical review and future directions for research. *Information Management & Computer Security*, Vol. 22, No. 3, pp. 279–308.

Siponen, M.; **Willison, R. (2009):** Information security management standards: Problems and solutions. *Information & Management*, Vol. 46, No. 5, pp. 267–270.

SJR (2018): SJR: Scientific journal rankings. `https://www.scimagojr.com/journalrank.php`, last accessed 2020-03-02.

Smith, S.; **Winchester, D.**; **Bunker, D.**; **Jaimeson, R. (2010):** Circuits of power: A study of mandated compliance to an information systems security de jure standard in a government organization. *MIS Quarterly*, Vol. 34, No. 3, pp. 463–486.

Solis, B. (2018): The State of Digital Transformation. Altimeter, a Prophet Company, Technical Report.

Sommestad, T.; **Hallberg, J.**; **Lundholm, K.**; **Bengtsson, J. (2014):** Variables influencing information security policy compliance: A systematic review of quantitative studies. *Information Management & Computer Security*, Vol. 22, No. 1, pp. 42–75.

Sonnenberg, C.; **Vom Brocke, J. (2012):** Evaluation patterns for design science research artefacts. *In Practical Aspects of Design Science*,Vol. 286, Berlin, Heidelberg, Springer Berlin Heidelberg, pp. 71–83.

Soomro, Z. A.; **Shah, M. H.**; **Ahmed, J. (2016):** Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, Vol. 36, No. 2, pp. 215–225.

Sowa, S.; **Gabriel, R. (2009):** Multidimensional management of information security: A metrics based approach merging business and information security topics. *In International Conference on Availability, Reliability and Security*, Fukuoka, Japan, pp. 750–755.

Speier-Pero, C. (2019): Using aggregated data under time pressure: a mechanism for coping with information overload. *Journal of Decision Systems*, Vol. 28, No. 2, pp. 82–100.

Straub, D. W.; **Welke, R. J. (1998):** Coping with systems risk: security planning models for management decision making. *MIS Quarterly*, Vol. 22, No. 4, pp. 441–469.

Sun, K.; **Jajodia, S.**; **Li, J.**; **Cheng, Y.**; **Tang, W.**; **Singhal, A. (2011):** Automatic security analysis using security metrics. *In MILCOM 2011 Military Communications Conference*, Baltimore, MD, USA, IEEE, pp. 1207–1212.

Sunyaev, A.; **Tremmel, F.**; **Mauro, C.**; **Leimeister, J. M. & Krcmar, H. (2009):** A re-classification of IS security analysis approaches. *In 15th Americas Conference on Information Systems*, San Francisco, CA, USA.

Tang, L. C.; **Zhao, Y.**; **Austin, S.**; **Darlington, M.**; **Culley, S. (2010):** Codification vs personalisation: A study of the information evaluation practice between aerospace and construction industries. *International Journal of Information Management*, Vol. 30, No. 4, pp. 315–325.

Tanna, G. B.; **Gupta, M.**; **Rao, H. R.**; **Upadhyaya, S. (2005):** Information assurance metric development framework for electronic bill presentment and payment systems using transaction and workflow analysis. *Decision Support Systems*, Vol. 41, No. 1, pp. 242–261.

Tariq, M. I. (2012): Towards information security metrics framework for cloud computing. *International Journal of Cloud Computing and Services Science (IJ-CLOSER)*, Vol. 1, No. 4, pp. 209–217.

Tashi, I.; **Ghernaouti-Hélie, S. (2008):** Efficient security measurements and metrics for risk assessment. *In 3rd International Conference on Internet Monitoring and Protection*, Bucharest, Romania, pp. 131–138.

Tewamba, H. N.; **Kamdjoug, J. R. K.**; **Bitjoka, G. B.**; **Wamba, S. F.**; **Bahanag, N. N. M. (2019):** Effects of information security management systems on firm performance. *American Journal of Operations Management and Information Systems*, Vol. 4, No. 3, pp. 99–108.

Thycopic Software Ltd. (2017): The 2017 state of cybersecurity metrics annual report. Thycopic Software Ltd., Technical Report.

Torres, J. M.; **Sarriegi, J. M.**; **Santos, J.**; **Serrano, N. (2006):** Managing information systems security: Critical success factors and indicators to measure effectiveness. *Information Security. ISC 2006. Lecture Notes in Computer Science*, Vol. 4176, pp. 530–545.

Tran, H.; **Campos-Nanez, E.**; **Fomin, P.**; **Wasek, J. (2016):** Cyber resilience recovery model to combat zero-day malware attacks. *Computers & Security*, Vol. 61, pp. 19–31.

Trèek, D. (2003): An integral framework for information systems security management. *Computers & Security*, Vol. 22, No. 4, pp. 337–360.

Tsiakis, T.; **Stephanides, G. (2005):** The economic approach of information security. *Computers & Security*, Vol. 24, No. 2, pp. 105–108.

Tsoukiàs, A. (2008): From decision theory to decision aiding methodology. *European Journal of Operational Research*, Vol. 187, No. 1, pp. 138–161.

Tu, C. Z.; **Yuan, Y.**; **Archer, N.**; **Connelly, C. E. (2018):** Strategic value alignment for information security management: A critical success factor analysis. *Information and Computer Security*, Vol. 26, No. 2, pp. 150–170.

Tu, Z.; **Yuan, Y. (2014):** Critical success factors analysis on effective information security management: A literature review. *In 20th Americas Conference on Information Systems*, Savannah, Georgia, USA, pp. 1874–1886.

Uffen, J.; **Breitner, M. H. (2013):** Management of technical security measures: An empirical examination of personality traits and behavioral intentions. *In 46th Hawaii International Conference on System Sciences*, Big Island, HI, USA, pp. 4551–4560.

Vance, A.; **Eargle, D.**; **Anderson, B. B.**; **Kirwan, C. B. (2014):** Using measures of risk perception to predict information security behavior: Insights from electroencephalography (EEG). *Journal of the Association for Information Systems*, Vol. 15, pp. 679–722.

Vaughn, R. B.; **Henning, R.**; **Siraj, A. (2003):** Information assurance measures and metrics – state of practice and proposed taxonomy. *In 36th Annual Hawaii International Conference on System Sciences*, Big Island, HI, USA.

Veiga, A. D.; **Eloff, J. H. P. (2007):** An information security governance framework. *Information Systems Management*, Vol. 24, No. 4, pp. 361–372.

Velki, T.; **Solic, K.**; **Ocevcic, H. (2014):** Development of users' information security awareness questionnaire (UISAQ) – Ongoing work. *In 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, Opatija, Croatia, pp. 1417–1421.

Verendel, V. (2009): Quantified security is a weak hypothesis: A critical survey of results and assumptions. *In 2009 workshop on New security paradigms workshop*, Oxford, UK, pp. 37—50.

Verizon Communications Inc. (2019): 2019 data breach investigations report. Verizon Communications Inc., Technical Report.

Vessey, I. (1994): The effect of information presentation on decision making: A cost-benefit analysis. *Information & Management*, Vol. 27, No. 2, pp. 103–119.

vom Brocke, J.; **Simons, A.**; **Niehaves, B.**; **Riemer, K.**; **Plattfaut, R.**; **Cleven, A. (2009):** Reconstructing the giant: On the importance of rigour in documenting the literature search process. *In 17th European Conference on Information Systems (ECIS)*, Verona, Italy, pp. 2206–2217.

von Solms, B.; **von Solms, R. (2004):** The 10 deadly sins of information security management. *Computers & Security*, Vol. 23, No. 5, pp. 371–376.

von Solms, R.; **van der Haar, H.**; **von Solms, S. H.**; **Caelli, W. J. (1994):** A framework for information security evaluation. *Information & Management*, Vol. 26, No. 3, pp. 143–153.

von Solms, R.; **van Niekerk, J. (2013):** From information security to cyber security. *Computers & Security*, Vol. 38, pp. 97–102.

Wang, C.; **Wulf, W. A. (1997):** Towards a framework for security measurement. *In 20th National Information Systems Security Conference*, Baltimore, Maryland, USA, pp. 522–533.

Wang, T.; **Kannan, K. N.**; **Ulmer, J. R. (2013):** The association between the disclosure and the realization of information security risk factors. *Information Systems Research*, Vol. 24, No. 2, pp. 201–218.

Webster, J.; **Watson, R. T. (2002):** Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, Vol. 26, No. 2, pp. xiii–xxiii.

Whitman, M. E.; **Mattord, H. J. (2012):** Principles of information security. 4. Edition. Stamford, Course Technology, Cengage Learning.

Wilkin, C. L.; **Chenhall, R. H. (2010):** A review of IT governance: A taxonomy to inform accounting information systems. *Journal of Information Systems*, Vol. 24, No. 2, pp. 107–146.

Wilkinson, S. (2004): 10 Focus Group Research. *In* **Silverman, D. e. ed.:** *Qualitative research: Theory, method and practice, 2nd ed*, Sage, pp. 177–199.

Willison, R.; **Backhouse, J. (2006):** Opportunities for computer crime: Considering systems risk from a criminological perspective. *European Journal of Information Systems*, Vol. 15, No. 4, pp. 403–414.

Wolfswinkel, J. F.; **Furtmueller, E.**; **Wilderom, C. P. M. (2013):** Using grounded theory as a method for rigorously reviewing literature. *European Journal of Information Systems*, Vol. 22, No. 1, 45–55.

Wood, C. C. (1987): Information systems security: Management success factors. *Computers & Security*, Vol. 6, No. 4, pp. 314–320.

Yaokumah, W. (2014): Information security governance implementation within ghanaian industry sectors. *Information Management & Computer Security*, Vol. 22, No. 3, pp. 235–250.

Yeh, Q.-J.; **Chang, A. J.-T. (2007):** Threats and countermeasures for information system security: A cross-industry study. *Information & Management*, Vol. 44, No. 5, pp. 480–491.

Yeniman Yildirim, E.; **Akalp, G.**; **Aytac, S.**; **Bayram, N. (2011):** Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey. *International Journal of Information Management*, Vol. 31, No. 4, pp. 360–365.

Yigitbasioglu, O. M.; **Velcu, O. (2012):** A review of dashboards in performance management: Implications for design and research. *International Journal of Accounting Information Systems*, Vol. 13, No. 1, pp. 41–59.

Young, D.; **Lopez, J.**; **Rice, M.**; **Ramsey, B.**; **McTasney, R. (2016):** A framework for incorporating insurance in critical infrastructure cyber risk strategies. *International Journal of Critical Infrastructure Protection*, Vol. 14, pp. 43–57.

Yulianto, S.; **Lim, C.**; **Soewito, B. (2016):** Information security maturity model: A best practice driven approach to PCI DSS compliance. *In 2016 IEEE Region 10 Symposium (TENSYMP)*, Bali, Indonesia, pp. 65–70.

Zalewski, J.; **Drager, S.**; **McKeever, W.**; **Kornecki, A. J. (2014):** Measuring security: A challenge for the generation. *In 2014 Federated Conference on Computer Science and Information Systems*, Warsaw, Poland, Annals of Computer Science and Information Systems, pp. 131–140.

Zang, W. L. (2014): Research of information security quantitative evaluation method. *Applied Mechanics and Materials*, Vol. 513-517, pp. 369–372.

Zerodium (2020): Our exploit acquisition program - Zerodium payouts. `https://zerodium.com/program.html`, Last accessed 2020-05-17.

Zobel, C. W.; **Khansa, L. (2012):** Quantifying cyberinfrastructure resilience against multi-event attacks. *Decision Sciences*, Vol. 43, No. 4, pp. 687–710.

Appendix

Appendix A: P2 - Literature Search Matrix

Resource	Hits	Relevant
MIS Quarterly	7	1
European Journal of Information Systems	20	3
Information Systems Journal	27	4
Information Systems Research	22	5
Journal of AIS	11	5
Journal of Information Technology	25	0
Journal of Management Information Systems	1	0
Journal of Strategic Information Systems	14	5
Journal of Management Information Systems	26	2
Decision Sciences	18	2
Information & Management	53	5
Information and Computer Security	99	10
IEEE Trans. on Dependable & Secure Computing	8	1
IEEE Trans. on Information Forensics and Security	7	0
Computers & Security	84	15
Google Scholar	100	11
ScienceDirect	41	6
OpacPlus	110	19
Backward		10
Forward		32
SUM	**673**	**136**

Table 1: *P2 - Literature Search Matrix*

Appendix B: P2 - Coding of the Literature to MSFs

First-order code	Second-order code	Cluster
technical vulnerabilities (Straub/Welke, 1998; Yeh/Chang, 2007; NIST, 2008; Premaratne et al., 2008; Tashi/Ghernaouti-Hélie, 2008; Boss et al., 2009; Dzazali/Sulaiman/Zolait, 2009; Kraemer/Carayon/Clem, 2009; Sowa/Gabriel, 2009; Sunyaev et al., 2009; Arora et al., 2010)	technical vulnerabilities	Vulnerability
vulnerability assessment (Wood, 1987; Coronado et al., 2009; Siponen/Willison, 2009; Jafari et al., 2010; Gosavi/Bagade, 2015)		
network vulnerability (Geer/Hoo/Jaquith, 2003; Idika/Bhargava, 2012; Gao/Zhong, 2015)		
system vulnerability (Jean Camp/Wolfram, 2004; Boyer/McQueen, 2007; Lee/Larsen, 2009; Pudar/Manimaran/Liu, 2009; Dogaheh, 2010; Hayden, 2010; Goldstein/Chernobai/Benaroch, 2011; Norman/Yasin, 2013; Holm/Afridi, 2015; Pendleton et al., 2017)		
vulnerability disclosure (Ransbotham/Mitra, 2009)		
host vulnerability (Idika/Bhargava, 2012)		
security problem (Straub/Welke, 1998)		
vulnerability (Vaughn/Henning/Siraj, 2003; Tanna et al., 2005; Herzog/Shahmehri/Duma, 2007; Johnson/Goetz, 2007; Yeh/Chang, 2007; Ashenden, 2008; Verendel, 2009; Leon/Saxena, 2010; Savola/Heinonen, 2011; Ben-Aissa et al., 2012; Crossler/Belanger, 2012; Hajdarevic et al., 2012; Ifinedo, 2012; Bayuk/Mostashari, 2013; Bayuk, 2013; Fenz et al., 2013; Hajdarevic/Allen, 2013; Hua/Bapna, 2013; Mermigas/Patsakis/Pirounias, 2013; von Solms/van Niekerk, 2013; Wang/Kannan/Ulmer, 2013; Fenz et al., 2014; Zalewski et al., 2014; Alqahtani, 2015; Mazur/Ksiezopolski/Kotulski, 2015; Nazareth/Choi, 2015; Posey/Roberts/Lowry, 2015; Alavi/Islam/Mouratidis, 2016; Muthukrishnan/Palaniappan, 2016; Young et al., 2016; Azuwa/Sahib/Shamsuddin, 2017)		
application security (Anderson/Moore, 2006; Yeh/Chang, 2007; Dzazali/Sulaiman/Zolait, 2009; Goel/Chengalur-Smith, 2010; Joh/Malaiya, 2011; Hajdarevic et al., 2012; Bayuk, 2013; Hajdarevic/Allen, 2013; Fenz et al., 2014; Mazur/Ksiezopolski/Kotulski, 2015; Mijnhardt/Baars/Spruit, 2016; Muthukrishnan/Palaniappan, 2016)	application security	
application defect (Geer/Hoo/Jaquith, 2003)		

feature security (Ransbotham/Mitra, 2009)		
patch coverage (Geer/Hoo/Jaquith, 2003; Ransbotham/Mitra, 2009; Arora et al., 2010; Joh/Malaiya, 2011; Crossler/Belanger, 2012; Bayuk, 2013; Muthukrishnan/Palaniappan, 2016; Pendleton et al., 2017)		
software problem (Gupta/Hammond, 2005)		
it security (Willison/Backhouse, 2006; Björck et al., 2015; Manhart/Thalmann, 2015)	technical security	
technology (Gonzalez/Sawicka, 2002; Trèek, 2003; Herrera, 2005; Katos/Adams, 2005; Ashenden, 2008; Merete Hagen/Albrechtsen/Hovden, 2008; Kraemer/Carayon/Clem, 2009; Goel/Chengalur-Smith, 2010; Jafari et al., 2010; Leon/Saxena, 2010; Goldstein/Chernobai/Benaroch, 2011; Hall/Sarkani/Mazzuchi, 2011; Norman/Yasin, 2013; AlHogail, 2015; Nazareth/Choi, 2015; Yulianto/Lim/Soewito, 2016)		
technical security (von Solms et al., 1994; Vaughn/Henning/Siraj, 2003; von Solms/von Solms, 2004; Savola, 2007; Veiga/Eloff, 2007; Coronado et al., 2009; Dinev et al., 2009; Sowa/Gabriel, 2009; Hedström et al., 2011; Savola/Heinonen, 2011; Hajdarevic et al., 2012; Ifinedo, 2012; Crossler et al., 2013; Uffen/Breitner, 2013; Fenz et al., 2014; Tu/Yuan, 2014; Gao/Zhong, 2015; Gosavi/Bagade, 2015; Manhart/Thalmann, 2015; Montesdioca/Maçada, 2015; Soomro/Shah/Ahmed, 2016; Azuwa/Sahib/Shamsuddin, 2017)		

Table 2: *Vulnerability*

First-order code	**Second-order code**	**Cluster**
physical security (von Solms et al., 1994; Wang/Wulf, 1997; Hong et al., 2003; Kankanhalli et al., 2003; Trèek, 2003; Ernest Chang/Ho, 2006; Willison/Backhouse, 2006; Dzazali/Sulaiman/Zolait, 2009; Pudar/Manimaran/Liu, 2009; Sowa/Gabriel, 2009; Goldstein/Chernobai/Benaroch, 2011; Hajdarevic et al., 2012; Hajdarevic/Allen, 2013; Norman/Yasin, 2013; Fenz et al., 2014; Narain Singh/Gupta/Ojha, 2014; Tu/Yuan, 2014; Gosavi/Bagade, 2015; Mazur/Ksiezopolski/Kotulski, 2015; Collier et al., 2016; Mijnhardt/Baars/Spruit, 2016)	physical security	Physical security
physical access (Trèek, 2003; LeMay et al., 2011)		
physical environment (Veiga/Eloff, 2007; Yeh/Chang, 2007; Jafari et al., 2010; Smith et al., 2010)		

Table 3: *Physical security*

First-order code	Second-order code	Cluster
organizational compliance (Jean Camp/Wolfram, 2004)	policy	Compliance & Policy
policy compliance (Hong et al., 2003; Trèek, 2003; Smith et al., 2010; Hall/Sarkani/Mazzuchi, 2011; Hu et al., 2012; Ifinedo, 2012; Crossler et al., 2013; Johnston et al., 2016)		
policy (Wood, 1987; von Solms et al., 1994; Straub/Welke, 1998; Hong et al., 2003; Vaughn/Henning/Siraj, 2003; Cavusoglu/Mishra/Raghunathan, 2004; Kotulic/Clark, 2004; Sharman/Rao/Upadhyaya, 2004; von Solms/von Solms, 2004; Herrera, 2005; Katos/Adams, 2005; Tsiakis/Stephanides, 2005; Ernest Chang/Ho, 2006; Willison/Backhouse, 2006; Johnson/Goetz, 2007; Veiga/Eloff, 2007; Yeh/Chang, 2007; Ashenden, 2008; Merete Hagen/Albrechtsen/Hovden, 2008; Tashi/Ghernaouti-Hélie, 2008; Boss et al., 2009; Dzazali/Sulaiman/Zolait, 2009; Herath/Rao, 2009; Knapp et al., 2009; Kotenko/Bogdanov, 2009; Kraemer/Carayon/Clem, 2009; Ransbotham/Mitra, 2009; Abu-Musa, 2010; Goel/Chengalur-Smith, 2010; Hayden, 2010; Jafari et al., 2010; Hedström et al., 2011; Mishra/Chasalow, 2011; Idika/Bhargava, 2012; Bayuk/Mostashari, 2013; Norman/Yasin, 2013; Uffen/Breitner, 2013; Wang/Kannan/Ulmer, 2013; Narain Singh/Gupta/Ojha, 2014; Tu/Yuan, 2014; Lowry/Moody, 2015; Montesdioca/Maçada, 2015; Nazareth/Choi, 2015; Alavi/Islam/Mouratidis, 2016; Mijnhardt/Baars/Spruit, 2016; Soomro/Shah/Ahmed, 2016; Horne/Maynard/Ahmad, 2017)		
security compliance (Sharman/Rao/Upadhyaya, 2004; Ernest Chang/Ho, 2006; Willison/Backhouse, 2006; Dzazali/Sulaiman/Zolait, 2009; Herath/Rao, 2009; Kraemer/Carayon/Clem, 2009; Hayden, 2010; Karjalainen/Siponen, 2011; Ifinedo, 2012; Crossler et al., 2013; Fenz et al., 2013; Fenz et al., 2014; Narain Singh/Gupta/Ojha, 2014; Tu/Yuan, 2014; Lowry/Moody, 2015; Mijnhardt/Baars/Spruit, 2016; Soomro/Shah/Ahmed, 2016; Yulianto/Lim/Soewito, 2016)		
legal requirements (von Solms/von Solms, 2004; Dzazali/Sulaiman/Zolait, 2009; Knapp et al., 2009; Kraemer/Carayon/Clem, 2009; Sunyaev et al., 2009; Savola/Heinonen, 2011; Uffen/Breitner, 2013; Manhart/Thalmann, 2015; Alavi/Islam/Mouratidis, 2016)	compliance	

law compliance (Hong et al., 2003; Johnson/Goetz, 2007; Veiga/Eloff, 2007; Yeh/Chang, 2007; Merete Hagen/Albrechtsen/Hovden, 2008; Leon/Saxena, 2010; Hall/Sarkani/Mazzuchi, 2011; Tariq, 2012)		
legislation (Trèek, 2003; Tashi/Ghernaouti-Hélie, 2008)		
regulatory requirements (Abu-Musa, 2010; Bayuk/ Mostashari, 2013; Fenz et al., 2013; Norman/Yasin, 2013; Atoum/Otoom/Abu Ali, 2014)		
regulatory compliance (Narain Singh/Gupta/Ojha, 2014; Horne/Maynard/Ahmad, 2017)		

Table 4: *Compliance & Policy*

First-order code	**Second-order code**	**Cluster**
risk management (von Solms et al., 1994; Straub/ Welke, 1998; Geer/Hoo/Jaquith, 2003; Kotulic/ Clark, 2004; Ernest Chang/Ho, 2006; Savola, 2007; Yeh/Chang, 2007; Ashenden, 2008; Merete Hagen/Albrechtsen/Hovden, 2008; NIST, 2008; Coronado et al., 2009; Ransbotham/Mitra, 2009; Savola, 2009; Sowa/Gabriel, 2009; Beresnevichiene/Pym/Shiu, 2010; Leon/Saxena, 2010; Wilkin/Chenhall, 2010; Hall/ Sarkani/Mazzuchi, 2011; Savola/Heinonen, 2011; Hajdarevic et al., 2012; Bayuk/Mostashari, 2013; Bayuk, 2013; Fenz et al., 2013; Hajdarevic/Allen, 2013; Norman/Yasin, 2013; Wang/Kannan/Ulmer, 2013; Fenz et al., 2014; Tu/Yuan, 2014; Yaokumah, 2014; Gao/Zhong, 2015; Lowry/Moody, 2015; Manhart/ Thalmann, 2015; Mazur/Ksiezopolski/Kotulski, 2015; Nazareth/Choi, 2015; Collier et al., 2016; Mijnhardt/ Baars/Spruit, 2016; Horne/Maynard/Ahmad, 2017)	risk management	Risk
risk analysis (Tsiakis/Stephanides, 2005; Kumar/Park/Subramaniam, 2008; Pudar/Manimaran/ Liu, 2009; Sunyaev et al., 2009; Goel/Chengalur-Smith, 2010; Zobel/Khansa, 2012; Hua/Bapna, 2013; Young et al., 2016)		
risk prevention (Veiga/Eloff, 2007; Hall/Sarkani/ Mazzuchi, 2011)		
risk tolerance (Liang/Xue, 2009)		
risk exposure (Mermigas/Patsakis/Pirounias, 2013)		
risk prediction (Fenz et al., 2014)		
software risk (Tanna et al., 2005; Boss et al., 2009)		
system risk (Willison/Backhouse, 2006; Chai/Kim/ Rao, 2011; Pendleton et al., 2017)		
risk perception (Vance et al., 2014)		

risk assessment (von Solms et al., 1994; Straub/Welke, 1998; Gonzalez/Sawicka, 2002; Hong et al., 2003; Jean Camp/Wolfram, 2004; Cavusoglu/Mishra/Raghunathan, 2004; Johnson/Goetz, 2007; Veiga/Eloff, 2007; Tashi/Ghernaouti-Hélie, 2008; Knapp et al., 2009; Siponen/Willison, 2009; Sunyaev et al., 2009; Verendel, 2009; Abu-Musa, 2010; Dogaheh, 2010; Hayden, 2010; Chai/Kim/Rao, 2011; Goldstein/Chernobai/Benaroch, 2011; Joh/Malaiya, 2011; Fenz et al., 2014; Gosavi/Bagade, 2015; Alavi/Islam/Mouratidis, 2016; Azuwa/Sahib/Shamsuddin, 2017)		
local threats (Willison/Backhouse, 2006)	threats	
threat impact (Alqahtani, 2015; Holm/Afridi, 2015)		
available exploits (Premaratne et al., 2008; Holm/Afridi, 2015)		
possible threats (Trèek, 2003; Gupta/Hammond, 2005; Tsiakis/Stephanides, 2005; Herzog/Shahmehri/Duma, 2007; Boss et al., 2009; Coronado et al., 2009; Knapp et al., 2009; Lee/Larsen, 2009; Sowa/Gabriel, 2009; Sunyaev et al., 2009; Verendel, 2009; Abu-Musa, 2010; Dogaheh, 2010; Jafari et al., 2010; Hall/Sarkani/Mazzuchi, 2011; Purboyo/Rahardjo/Kuspriyanto, 2011; Ben-Aissa et al., 2012; Crossler/Belanger, 2012; Hajdarevic et al., 2012; Hu et al., 2012; Ifinedo, 2012; Jones/Horowitz, 2012; Tariq, 2012; Zobel/Khansa, 2012; Bayuk/Mostashari, 2013; Bayuk, 2013; Crossler et al., 2013; Fenz et al., 2013; Hajdarevic/Allen, 2013; Hua/Bapna, 2013; Norman/Yasin, 2013; Uffen/Breitner, 2013; von Solms/van Niekerk, 2013; Fenz et al., 2014; Herath et al., 2014; Tu/Yuan, 2014; Alqahtani, 2015; Gao/Zhong, 2015; Gosavi/Bagade, 2015; Mazur/Ksiezopolski/Kotulski, 2015; Nazareth/Choi, 2015; Posey/Roberts/Lowry, 2015; Collier et al., 2016; Johnston et al., 2016; Muthukrishnan/Palaniappan, 2016; Tran et al., 2016; Young et al., 2016; Azuwa/Sahib/Shamsuddin, 2017; Pendleton et al., 2017)		

Table 5: *Risk*

First-order code	**Second-order code**	**Cluster**
resilience (Johnson/Goetz, 2007; Zobel/Khansa, 2012; Fenz et al., 2013; Zalewski et al., 2014; Björck et al., 2015; Collier et al., 2016; Tran et al., 2016)	it continuity	Continuity
power failure (Gupta/Hammond, 2005)		

survivability (Vaughn/Henning/Siraj, 2003; Katos/ Adams, 2005)		
contingency plan (Wood, 1987; von Solms et al., 1994; Abu-Musa, 2010)		
acts of god (Willison/Backhouse, 2006; Björck et al., 2015)		
natural disaster (Gupta/Hammond, 2005)		
business continuity (Hong et al., 2003; Trèek, 2003; Veiga/Eloff, 2007; Tashi/Ghernaouti-Hélie, 2008; Dzazali/Sulaiman/Zolait, 2009; Sowa/Gabriel, 2009; Smith et al., 2010; Narain Singh/Gupta/Ojha, 2014; Horne/Maynard/Ahmad, 2017)	business continuity	
business continuity plan (Ernest Chang/Ho, 2006; Tariq, 2012; Mijnhardt/Baars/Spruit, 2016)		
restorability (Boyer/McQueen, 2007; Bayuk/ Mostashari, 2013)	recovery	
disaster recovery (von Solms et al., 1994; Kumar/Park/Subramaniam, 2008; Savola, 2009; Wilkin/Chenhall, 2010; Hall/Sarkani/Mazzuchi, 2011; Crossler/Belanger, 2012; Tariq, 2012)		

Table 6: *Continuity*

First-order code	**Second-order code**	**Cluster**
infrastructure administration (Wood, 1987; Savola/Heinonen, 2011; Hua/Bapna, 2013)	infrastructure overview	Infrastructure
secure environment (Wood, 1987; von Solms et al., 1994; Gonzalez/Sawicka, 2002; Trèek, 2003; Herrera, 2005; Ernest Chang/Ho, 2006; Herath/Rao, 2009; Liang/Xue, 2009; Abu-Musa, 2010; Norman/Yasin, 2013; Narain Singh/Gupta/Ojha, 2014; AlHogail, 2015; Posey/Roberts/Lowry, 2015; Mijnhardt/Baars/Spruit, 2016)		
infrastructure security (Hong et al., 2003; Trèek, 2003; Katos/Adams, 2005; Crossler/Belanger, 2012)		
ict infrastructure (Cavusoglu/Mishra/Raghunathan, 2004; Fenz et al., 2013; Soomro/Shah/Ahmed, 2016; Horne/Maynard/Ahmad, 2017)		
equipment (Sharman/Rao/Upadhyaya, 2004)		
hardware security (Yeh/Chang, 2007)		
network security (Kotenko/Bogdanov, 2009; Bayuk/ Mostashari, 2013; Bayuk, 2013; Gosavi/Bagade, 2015; Mazur/Ksiezopolski/Kotulski, 2015; Azuwa/Sahib/ Shamsuddin, 2017)	network security	
network hardening (Idika/Bhargava, 2012)		

secure network communication (Herzog/ Shahmehri/Duma, 2007; Yeh/Chang, 2007; Premaratne et al., 2008; Ransbotham/Mitra, 2009; Smith et al., 2010; Fenz et al., 2014; Azuwa/ Sahib/Shamsuddin, 2017)		
cryptography (Wang/Wulf, 1997; Geer/Hoo/Jaquith, 2003; Trèek, 2003; Herzog/Shahmehri/Duma, 2007)		
encryption (Gupta/Hammond, 2005; Chai/Kim/Rao, 2011; Ifinedo, 2012; Gosavi/Bagade, 2015)		
secure protocol (Ransbotham/Mitra, 2009)		
asset identification (Trèek, 2003; Sharman/Rao/ Upadhyaya, 2004; Ernest Chang/Ho, 2006; Merete Hagen/Albrechtsen/Hovden, 2008; NIST, 2008; Jafari et al., 2010; Bayuk/Mostashari, 2013; von Solms/ van Niekerk, 2013; Fenz et al., 2014)	asset knowledge	
asset assessment (Boyer/McQueen, 2007; Herzog/Shahmehri/Duma, 2007; Kraemer/Carayon/Clem, 2009; Jafari et al., 2010; Smith et al., 2010; Purboyo/ Rahardjo/Kuspriyanto, 2011; Hajdarevic et al., 2012; Gao/Zhong, 2015; Montesdioca/Maçada, 2015)		
asset management (Hong et al., 2003; Veiga/Eloff, 2007; Smith et al., 2010; Hall/Sarkani/Mazzuchi, 2011; Ifinedo, 2012; Crossler et al., 2013; Mijnhardt/Baars/ Spruit, 2016; Soomro/Shah/Ahmed, 2016; Horne/ Maynard/Ahmad, 2017)		
asset classification (Narain Singh/Gupta/Ojha, 2014)		
system configuration (Geer/Hoo/Jaquith, 2003; Kotenko/Bogdanov, 2009; Kraemer/Carayon/Clem, 2009; Jafari et al., 2010; Leon/Saxena, 2010; Jones/ Horowitz, 2012; Bayuk, 2013; Hua/Bapna, 2013; Alavi/ Islam/Mouratidis, 2016; Muthukrishnan/Palaniappan, 2016)	system hardening	
system maintenance (Wood, 1987; Hong et al., 2003; Trèek, 2003; Ernest Chang/Ho, 2006; Veiga/Eloff, 2007; NIST, 2008; Sowa/Gabriel, 2009; Smith et al., 2010; Ifinedo, 2012; Narain Singh/Gupta/Ojha, 2014; Nazareth/Choi, 2015; Alavi/Islam/Mouratidis, 2016)		
system weakness (Vaughn/Henning/Siraj, 2003; Goldstein/Chernobai/Benaroch, 2011; LeMay et al., 2011; Purboyo/Rahardjo/Kuspriyanto, 2011)		
connections with public network (Sharman/Rao/ Upadhyaya, 2004; Johnson/Goetz, 2007)	external connections	
access points (NIST, 2008)		
external system connections (Pudar/Manimaran/ Liu, 2009; von Solms/van Niekerk, 2013)		

technology architecture (Cavusoglu/Mishra/Raghunathan, 2004; Johnson/Goetz, 2007; Knapp et al., 2009; Björck et al., 2015; Mijnhardt/Baars/Spruit, 2016)	architectural factors	
firewall architecture (Sharman/Rao/Upadhyaya, 2004)		
system architecture (Yeh/Chang, 2007; Jones/Horowitz, 2012; Soomro/Shah/Ahmed, 2016)		

Table 7: *Infrastructure*

First-order code	**Second-order code**	**Cluster**
identity (Wang/Wulf, 1997; Savola/Heinonen, 2011; Gosavi/Bagade, 2015; Mijnhardt/Baars/Spruit, 2016)	identity management	Access control
account management (Anderson/Moore, 2006; Osvaldo De Sordi/Meireles/Carvalho de Azevedo, 2014)		
access control (Geer/Hoo/Jaquith, 2003; Hong et al., 2003; Trèek, 2003; Dhillon/Torkzadeh, 2006; Ernest Chang/Ho, 2006; Willison/Backhouse, 2006; Boyer/McQueen, 2007; Herzog/Shahmehri/Duma, 2007; Veiga/Eloff, 2007; Dzazali/Sulaiman/Zolait, 2009; Ransbotham/Mitra, 2009; Abu-Musa, 2010; Beresnevichiene/Pym/Shiu, 2010; Dogaheh, 2010; Jafari et al., 2010; Chai/Kim/Rao, 2011; Crossler/Belanger, 2012; Ifinedo, 2012; Bayuk/Mostashari, 2013; Narain Singh/Gupta/Ojha, 2014; Holm/Afridi, 2015; Mijnhardt/Baars/Spruit, 2016; Azuwa/Sahib/Shamsuddin, 2017)	access control	
access rights (Sharman/Rao/Upadhyaya, 2004)		
software access control (Wang/Wulf, 1997; Smith et al., 2010; LeMay et al., 2011)		

Table 8: *Access control*

First-order code	**Second-order code**	**Cluster**
personnel security (von Solms et al., 1994; Kankanhalli et al., 2003; Trèek, 2003; Vaughn/Henning/Siraj, 2003; von Solms/von Solms, 2004; Herrera, 2005; Ernest Chang/Ho, 2006; Yeh/Chang, 2007; Herath/Rao, 2009; Ransbotham/Mitra, 2009; Sowa/Gabriel, 2009; Goel/Chengalur-Smith, 2010; Smith et al., 2010; Uffen/Breitner, 2013; Narain Singh/Gupta/Ojha, 2014)	awareness	Awareness

awareness (Straub/Welke, 1998; Hong et al., 2003; Kankanhalli et al., 2003; Sharman/Rao/Upadhyaya, 2004; von Solms/von Solms, 2004; Dhillon/Torkzadeh, 2006; Willison/Backhouse, 2006; Johnson/Goetz, 2007; Veiga/Eloff, 2007; Yeh/Chang, 2007; Ashenden, 2008; Merete Hagen/Albrechtsen/Hovden, 2008; Coronado et al., 2009; Dinev et al., 2009; Dzazali/Sulaiman/Zolait, 2009; Knapp et al., 2009; Kraemer/Carayon/Clem, 2009; Sowa/Gabriel, 2009; Abu-Musa, 2010; Jafari et al., 2010; Wilkin/Chenhall, 2010; Hall/Sarkani/Mazzuchi, 2011; Karjalainen/Siponen, 2011; Zobel/Khansa, 2012; Norman/Yasin, 2013; Wang/Kannan/Ulmer, 2013; Atoum/Otoom/Abu Ali, 2014; Narain Singh/Gupta/Ojha, 2014; Tu/Yuan, 2014; Velki/Solic/Ocevcic, 2014; Alqahtani, 2015; Gao/Zhong, 2015; Manhart/Thalmann, 2015; Alavi/Islam/Mouratidis, 2016; Soomro/Shah/Ahmed, 2016; Tran et al., 2016; Pendleton et al., 2017)		
people (Gonzalez/Sawicka, 2002; Sharman/Rao/Upadhyaya, 2004; Hall/Sarkani/Mazzuchi, 2011; Al-Hogail, 2015; Yulianto/Lim/Soewito, 2016; Horne/Maynard/Ahmad, 2017)		
technology awareness (Dinev/Hu, 2007; Herath et al., 2014)		
training (Sharman/Rao/Upadhyaya, 2004; Ashenden, 2008; Merete Hagen/Albrechtsen/Hovden, 2008; NIST, 2008; Dogaheh, 2010; Karjalainen/Siponen, 2011; Al-Hogail, 2015; Lowry/Moody, 2015; Posey/Roberts/Lowry, 2015; Tran et al., 2016)	user knowledge	
skills (Alavi/Islam/Mouratidis, 2016)		
user knowledge (Wood, 1987; Johnson/Goetz, 2007; Veiga/Eloff, 2007; Abu-Musa, 2010; Hajdarevic et al., 2012; Fenz et al., 2014; Alqahtani, 2015; Lowry/Moody, 2015; Manhart/Thalmann, 2015; Nazareth/Choi, 2015; Posey/Roberts/Lowry, 2015; Horne/Maynard/Ahmad, 2017)		
education (Willison/Backhouse, 2006; Kraemer/Carayon/Clem, 2009)		
it competence (Ernest Chang/Ho, 2006; Tu/Yuan, 2014)		
user activities (Geer/Hoo/Jaquith, 2003; Vance et al., 2014; Björck et al., 2015)	behavior	
human interaction (Trèek, 2003; Kotenko/Bogdanov, 2009)		
human error (Vaughn/Henning/Siraj, 2003; Kraemer/Carayon/Clem, 2009; Alavi/Islam/Mouratidis, 2016)		

user/human behavior (Gonzalez/Sawicka, 2002; Dinev/Hu, 2007; Veiga/Eloff, 2007; Merete Hagen/Albrechtsen/Hovden, 2008; Boss et al., 2009; Dinev et al., 2009; Herath/Rao, 2009; Kraemer/Carayon/Clem, 2009; Liang/Xue, 2009; Sowa/Gabriel, 2009; Dogaheh, 2010; Hedström et al., 2011; Karjalainen/Siponen, 2011; Ifinedo, 2012; Crossler et al., 2013; Hua/Bapna, 2013; Uffen/Breitner, 2013; von Solms/van Niekerk, 2013; Narain Singh/Gupta/Ojha, 2014; Vance et al., 2014; Velki/Solic/Ocevcic, 2014; Lowry/Moody, 2015; Montesdioca/Maçada, 2015; Johnston et al., 2016; Soomro/Shah/Ahmed, 2016)		
user error (Gupta/Hammond, 2005)		
criminal behavior (Kankanhalli et al., 2003)		
attack behavior (Pudar/Manimaran/Liu, 2009; Gao/Zhong, 2015)		
ethical dimension (von Solms/von Solms, 2004)	ethical factors	
work ethic (Dhillon/Torkzadeh, 2006)		
ethical environment (Dhillon/Torkzadeh, 2006; Veiga/Eloff, 2007)		
work situation (Dhillon/Torkzadeh, 2006)		
security culture (Johnson/Goetz, 2007; Veiga/Eloff, 2007; Ashenden, 2008; Merete Hagen/Albrechtsen/Hovden, 2008; Boss et al., 2009; Dinev et al., 2009; Herath/Rao, 2009; Knapp et al., 2009; Kraemer/Carayon/Clem, 2009; Hu et al., 2012; Norman/Yasin, 2013; Narain Singh/Gupta/Ojha, 2014; Tu/Yuan, 2014; AlHogail, 2015; Alavi/Islam/Mouratidis, 2016; Collier et al., 2016)	culture	
philosophical culture (Yulianto/Lim/Soewito, 2016)		
personal privacy (Dhillon/Torkzadeh, 2006; Boss et al., 2009; Coronado et al., 2009; Savola, 2009; Dogaheh, 2010; Wilkin/Chenhall, 2010; Ben-Aissa et al., 2012; Tariq, 2012; Fenz et al., 2013)	personal security	
trust (Dhillon/Torkzadeh, 2006; Veiga/Eloff, 2007; Boss et al., 2009; Coronado et al., 2009; Dzazali/Sulaiman/Zolait, 2009; Sowa/Gabriel, 2009; Dogaheh, 2010; Tariq, 2012; Gao/Zhong, 2015; Lowry/Moody, 2015; Johnston et al., 2016; Horne/Maynard/Ahmad, 2017)		
personal needs (Dhillon/Torkzadeh, 2006)		
individual belief (Hu et al., 2012)		
individual impact (Norman/Yasin, 2013)		
usefulness / easy to use (Dinev/Hu, 2007; Dinev et al., 2009; Osvaldo De Sordi/Meireles/Carvalho de Azevedo, 2014)	usability	

usability (Dinev/Hu, 2007; Lee/Larsen, 2009; Verendel, 2009; Bayuk, 2013)		

Table 9: *Awareness*

First-order code	Second-order code	Cluster
reliability (Wang/Wulf, 1997; Verendel, 2009; Savola/ Heinonen, 2011; Ben-Aissa et al., 2012; Zalewski et al., 2014)	protection goals	CIA
authenticity (Wang/Wulf, 1997; Trèek, 2003; Katos/ Adams, 2005; Tsiakis/Stephanides, 2005; Savola, 2009; Jafari et al., 2010; Savola/Heinonen, 2011; Ben-Aissa et al., 2012; Gosavi/Bagade, 2015; Holm/Afridi, 2015; Azuwa/Sahib/Shamsuddin, 2017)		
accountability (Wood, 1987; Dhillon/Torkzadeh, 2006; Leon/Saxena, 2010)		
non-repudiation (Wang/Wulf, 1997; Trèek, 2003; Tsiakis/Stephanides, 2005; Savola, 2009; Jafari et al., 2010; Purboyo/Rahardjo/Kuspriyanto, 2011; Ben-Aissa et al., 2012)		
data integrity (Gupta/Hammond, 2005; Dhillon/ Torkzadeh, 2006; Boyer/McQueen, 2007; Tariq, 2012)	integrity	
transaction integrity (Gupta/Hammond, 2005)		
process/organizational integrity (Dhillon/ Torkzadeh, 2006)		
integrity (Wang/Wulf, 1997; Hong et al., 2003; Trèek, 2003; Cavusoglu/Mishra/Raghunathan, 2004; Tsiakis/Stephanides, 2005; Ernest Chang/Ho, 2006; Ashenden, 2008; Tashi/Ghernaouti-Hélie, 2008; Dzazali/Sulaiman/Zolait, 2009; Knapp et al., 2009; Pudar/Manimaran/Liu, 2009; Savola, 2009; Sowa/ Gabriel, 2009; Abu-Musa, 2010; Beresnevichiene/Pym/ Shiu, 2010; Goel/Chengalur-Smith, 2010; Jafari et al., 2010; Leon/Saxena, 2010; Wilkin/Chenhall, 2010; Goldstein/Chernobai/Benaroch, 2011; Hall/Sarkani/ Mazzuchi, 2011; Hedström et al., 2011; Joh/Malaiya, 2011; Mishra/Chasalow, 2011; Purboyo/Rahardjo/ Kuspriyanto, 2011; Savola/Heinonen, 2011; Ben-Aissa et al., 2012; Hu et al., 2012; Tariq, 2012; Bayuk/ Mostashari, 2013; Hajdarevic/Allen, 2013; Hua/Bapna, 2013; Uffen/Breitner, 2013; von Solms/van Niekerk, 2013; Herath et al., 2014; Tu/Yuan, 2014; Yaokumah, 2014; Zalewski et al., 2014; Holm/Afridi, 2015; Nazareth/Choi, 2015; Posey/Roberts/Lowry, 2015; Mijnhardt/Baars/Spruit, 2016; Muthukrishnan/ Palaniappan, 2016; Horne/Maynard/Ahmad, 2017)		

available information (Dhillon/Torkzadeh, 2006)	availability	
availability (Wang/Wulf, 1997; Cavusoglu/Mishra/Raghunathan, 2004; Gupta/Hammond, 2005; Ernest Chang/Ho, 2006; Ashenden, 2008; Tashi/Ghernaouti-Hélie, 2008; Dzazali/Sulaiman/Zolait, 2009; Knapp et al., 2009; Kraemer/Carayon/Clem, 2009; Pudar/Manimaran/Liu, 2009; Savola, 2009; Sowa/Gabriel, 2009; Abu-Musa, 2010; Beresnevichiene/Pym/Shiu, 2010; Dogaheh, 2010; Goel/Chengalur-Smith, 2010; Jafari et al., 2010; Leon/Saxena, 2010; Goldstein/Chernobai/Benaroch, 2011; Hall/Sarkani/Mazzuchi, 2011; Hedström et al., 2011; Joh/Malaiya, 2011; Mishra/Chasalow, 2011; Purboyo/Rahardjo/Kuspriyanto, 2011; Ben-Aissa et al., 2012; Hu et al., 2012; Bayuk/Mostashari, 2013; Hajdarevic/Allen, 2013; Norman/Yasin, 2013; Uffen/Breitner, 2013; von Solms/van Niekerk, 2013; Herath et al., 2014; Tu/Yuan, 2014; Zalewski et al., 2014; Holm/Afridi, 2015; Nazareth/Choi, 2015; Posey/Roberts/Lowry, 2015; Mijnhardt/Baars/Spruit, 2016; Muthukrishnan/Palaniappan, 2016; Horne/Maynard/Ahmad, 2017)		
confidentiality (Wang/Wulf, 1997; Hong et al., 2003; Trèek, 2003; Cavusoglu/Mishra/Raghunathan, 2004; Tsiakis/Stephanides, 2005; Ernest Chang/Ho, 2006; Ashenden, 2008; Tashi/Ghernaouti-Hélie, 2008; Dzazali/Sulaiman/Zolait, 2009; Knapp et al., 2009; Pudar/Manimaran/Liu, 2009; Savola, 2009; Sowa/Gabriel, 2009; Abu-Musa, 2010; Beresnevichiene/Pym/Shiu, 2010; Dogaheh, 2010; Goel/Chengalur-Smith, 2010; Jafari et al., 2010; Leon/Saxena, 2010; Goldstein/Chernobai/Benaroch, 2011; Hall/Sarkani/Mazzuchi, 2011; Hedström et al., 2011; Joh/Malaiya, 2011; Mishra/Chasalow, 2011; Purboyo/Rahardjo/Kuspriyanto, 2011; Ben-Aissa et al., 2012; Hu et al., 2012; Bayuk/Mostashari, 2013; Hajdarevic/Allen, 2013; Uffen/Breitner, 2013; von Solms/van Niekerk, 2013; Herath et al., 2014; Osvaldo De Sordi/Meireles/Carvalho de Azevedo, 2014; Tu/Yuan, 2014; Yaokumah, 2014; Zalewski et al., 2014; Holm/Afridi, 2015; Nazareth/Choi, 2015; Posey/Roberts/Lowry, 2015; Mijnhardt/Baars/Spruit, 2016; Muthukrishnan/Palaniappan, 2016; Horne/Maynard/Ahmad, 2017)	confidentiality	

Table 10: *CIA*

First-order code	Second-order code	Cluster
organization size (Kankanhalli et al., 2003; Kotulic/Clark, 2004; Ernest Chang/Ho, 2006; Coronado et al., 2009; Lee/Larsen, 2009; Norman/Yasin, 2013; Narain Singh/Gupta/Ojha, 2014; Lowry/Moody, 2015)	organizational factors	Organizational factors
organizational factors (Hong et al., 2003; Trèek, 2003; Vaughn/Henning/Siraj, 2003; von Solms/von Solms, 2004; Savola, 2007; Veiga/Eloff, 2007; Herath/Rao, 2009; Kraemer/Carayon/Clem, 2009; Sowa/Gabriel, 2009; Sunyaev et al., 2009; Leon/Saxena, 2010; Fenz et al., 2014; Tu/Yuan, 2014; AlHogail, 2015; Manhart/Thalmann, 2015; Soomro/Shah/Ahmed, 2016)		
organization structure (Kotulic/Clark, 2004; Yeh/Chang, 2007; Abu-Musa, 2010; Atoum/Otoom/Abu Ali, 2014; Tu/Yuan, 2014)		
industry type (Kankanhalli et al., 2003; Ernest Chang/Ho, 2006; Yeh/Chang, 2007; Coronado et al., 2009; Dzazali/Sulaiman/Zolait, 2009; Norman/Yasin, 2013; Narain Singh/Gupta/Ojha, 2014)		
external conditions (Sharman/Rao/Upadhyaya, 2004)	external factor	
reputation (Osvaldo De Sordi/Meireles/Carvalho de Azevedo, 2014; Tu/Yuan, 2014; Gao/Zhong, 2015)		

Table 11: *Organizational factors*

First-order code	Second-order code	Cluster
countermeasures (measures) (Kotulic/Clark, 2004; Herzog/Shahmehri/Duma, 2007; Kumar/Park/Subramaniam, 2008; Tashi/Ghernaouti-Hélie, 2008; Pudar/Manimaran/Liu, 2009; Ransbotham/Mitra, 2009; Leon/Saxena, 2010; Crossler et al., 2013; Fenz et al., 2013; Mermigas/Patsakis/Pirounias, 2013; Fenz et al., 2014; Alavi/Islam/Mouratidis, 2016; Pendleton et al., 2017)	control development	Security management
control recommendation/implementation (Wood, 1987)		
safeguards (Willison/Backhouse, 2006; Tashi/Ghernaouti-Hélie, 2008; Dzazali/Sulaiman/Zolait, 2009; Liang/Xue, 2009; Ifinedo, 2012; Fenz et al., 2014; Yulianto/Lim/Soewito, 2016)		

security control (Hong et al., 2003; Cavusoglu/Mishra/Raghunathan, 2004; Tsiakis/Stephanides, 2005; Johnson/Goetz, 2007; Savola, 2007; Ashenden, 2008; Knapp et al., 2009; Siponen/Willison, 2009; Sowa/Gabriel, 2009; Sunyaev et al., 2009; Leon/Saxena, 2010; Goldstein/Chernobai/Benaroch, 2011; Hedström et al., 2011; Savola/Heinonen, 2011; Jones/Horowitz, 2012; Zobel/Khansa, 2012; Bayuk/Mostashari, 2013; Fenz et al., 2013; Hajdarevic/Allen, 2013; Atoum/Otoom/Abu Ali, 2014; Narain Singh/Gupta/Ojha, 2014; Zalewski et al., 2014; Lowry/Moody, 2015; Mazur/Ksiezopolski/Kotulski, 2015; Alavi/Islam/Mouratidis, 2016; Collier et al., 2016; Young et al., 2016; Azuwa/Sahib/Shamsuddin, 2017; Horne/Maynard/Ahmad, 2017)		
incident response (Jean Camp/Wolfram, 2004; Veiga/Eloff, 2007; Sowa/Gabriel, 2009; Abu-Musa, 2010; Jafari et al., 2010; Hall/Sarkani/Mazzuchi, 2011; Hajdarevic et al., 2012; Ifinedo, 2012; Bayuk/Mostashari, 2013; Alqahtani, 2015; Alavi/Islam/Mouratidis, 2016)	incident management	
incident handling (Sharman/Rao/Upadhyaya, 2004; Johnson/Goetz, 2007)		
compromise detection (Boyer/McQueen, 2007; Savola, 2007; Ransbotham/Mitra, 2009)		
breach investigation (Wood, 1987)		
incident management (Narain Singh/Gupta/Ojha, 2014; Mijnhardt/Baars/Spruit, 2016; Muthukrishnan/Palaniappan, 2016; Tran et al., 2016)		
fraud detection (Goldstein/Chernobai/Benaroch, 2011; Tran et al., 2016)		
compliance check (Wood, 1987)	monitor and check	
evaluation (measurement) (Wood, 1987; Savola, 2013; Tu/Yuan, 2014; Yaokumah, 2014; Zalewski et al., 2014; Gosavi/Bagade, 2015; Azuwa/Sahib/Shamsuddin, 2017; Pendleton et al., 2017)		
auditing (Trèek, 2003; Sharman/Rao/Upadhyaya, 2004; von Solms/von Solms, 2004; Katos/Adams, 2005; Ashenden, 2008; Knapp et al., 2009; Ransbotham/Mitra, 2009; Savola, 2009; Jafari et al., 2010; Leon/Saxena, 2010; Mishra/Chasalow, 2011; Bayuk/Mostashari, 2013; Atoum/Otoom/Abu Ali, 2014; Narain Singh/Gupta/Ojha, 2014; Azuwa/Sahib/Shamsuddin, 2017)		
certification (von Solms/von Solms, 2004; Savola, 2007; Veiga/Eloff, 2007; Sowa/Gabriel, 2009)		
surveillance (Sharman/Rao/Upadhyaya, 2004)		

monitoring (Sharman/Rao/Upadhyaya, 2004; Bayuk/ Mostashari, 2013; Savola, 2013; Mazur/Ksiezopolski/ Kotulski, 2015; Nazareth/Choi, 2015)		
operational processes (Trèek, 2003; Johnson/Goetz, 2007; Ashenden, 2008; Sowa/Gabriel, 2009; Hayden, 2010; Jafari et al., 2010)	operational rules	
administrative security (Kankanhalli et al., 2003; Yeh/Chang, 2007)		
procedures (Hong et al., 2003; Cavusoglu/Mishra/ Raghunathan, 2004; Kotulic/Clark, 2004; Tsiakis/ Stephanides, 2005; Veiga/Eloff, 2007; Merete Hagen/ Albrechtsen/Hovden, 2008; Tashi/Ghernaouti-Hélie, 2008; Boss et al., 2009; Dzazali/Sulaiman/Zolait, 2009; Herath/Rao, 2009; Hedström et al., 2011; Karjalainen/ Siponen, 2011; Osvaldo De Sordi/Meireles/Carvalho de Azevedo, 2014; Montesdioca/Maçada, 2015)		
processes (Vaughn/Henning/Siraj, 2003; Kotulic/ Clark, 2004; Tsiakis/Stephanides, 2005; Ransbotham/ Mitra, 2009; Abu-Musa, 2010; Goel/Chengalur-Smith, 2010; Goldstein/Chernobai/Benaroch, 2011; Hall/ Sarkani/Mazzuchi, 2011; Purboyo/Rahardjo/ Kuspriyanto, 2011; Hajdarevic et al., 2012; Bayuk/ Mostashari, 2013; Norman/Yasin, 2013; Zalewski et al., 2014; Mazur/Ksiezopolski/Kotulski, 2015; Montesdioca/Maçada, 2015; Yulianto/Lim/Soewito, 2016; Horne/ Maynard/Ahmad, 2017)		
operational readiness(Vaughn/Henning/Siraj, 2003)		
process documentation (Sowa/Gabriel, 2009; Yulianto/Lim/Soewito, 2016)		
standards (best practices) (von Solms/von Solms, 2004; Knapp et al., 2009; Sunyaev et al., 2009; Abu-Musa, 2010; Leon/Saxena, 2010; Smith et al., 2010; Goldstein/Chernobai/Benaroch, 2011; Hajdarevic et al., 2012; Fenz et al., 2013; Hajdarevic/Allen, 2013; Mermigas/Patsakis/Pirounias, 2013; Norman/ Yasin, 2013; Uffen/Breitner, 2013; Wang/Kannan/ Ulmer, 2013; Tu/Yuan, 2014; Mijnhardt/Baars/Spruit, 2016; Yulianto/Lim/Soewito, 2016; Azuwa/Sahib/ Shamsuddin, 2017)	standards	
governance (Kotulic/Clark, 2004; von Solms/von Solms, 2004; Knapp et al., 2009; Abu-Musa, 2010; Norman/Yasin, 2013; Atoum/Otoom/Abu Ali, 2014; Yaokumah, 2014; Horne/Maynard/Ahmad, 2017)		
ISMS (Herrera, 2005; Savola, 2007; Hajdarevic et al., 2012; Hajdarevic/Allen, 2013; Mijnhardt/Baars/ Spruit, 2016; Azuwa/Sahib/Shamsuddin, 2017)		
management implementation (Ernest Chang/Ho, 2006)		

management system (Ashenden, 2008)		
communication management (Trèek, 2003; Dhillon/Torkzadeh, 2006; Johnson/Goetz, 2007; Veiga/Eloff, 2007; Kraemer/Carayon/Clem, 2009; Smith et al., 2010; Norman/Yasin, 2013; Narain Singh/Gupta/Ojha, 2014; AlHogail, 2015; Alavi/ Islam/Mouratidis, 2016)	communication	
security enforcement (Savola, 2009)		
deterrence (Mishra/Chasalow, 2011; Johnston et al., 2016)		
sanctions (Lowry/Moody, 2015; Johnston et al., 2016)		
responsibility (Wood, 1987; Dhillon/Torkzadeh, 2006; Dzazali/Sulaiman/Zolait, 2009; Kraemer/ Carayon/Clem, 2009; Sowa/Gabriel, 2009; Abu-Musa, 2010; Posey/Roberts/Lowry, 2015; Horne/Maynard/ Ahmad, 2017)	responsibility	
ownership (Dhillon/Torkzadeh, 2006; Sharman/Rao/ Upadhyaya, 2004; AlHogail, 2015)		

Table 12: *Security management*

First-order code	**Second-order code**	**Cluster**
cost (Geer/Hoo/Jaquith, 2003; Tashi/Ghernaouti-Hélie, 2008; Lee/Larsen, 2009; Liang/Xue, 2009; Verendel, 2009; Arora et al., 2010; Hayden, 2010; Jafari et al., 2010; LeMay et al., 2011; Mishra/Chasalow, 2011; Ben-Aissa et al., 2012; Ifinedo, 2012; Tariq, 2012; Zobel/Khansa, 2012; Nazareth/Choi, 2015; Alavi/Islam/ Mouratidis, 2016)	investment balance	Resources
cost-benefit/effectiveness (Gonzalez/Sawicka, 2002; Cavusoglu/Mishra/Raghunathan, 2004; Savola, 2007; Ransbotham/Mitra, 2009; Sowa/Gabriel, 2009)		
possible cost (Trèek, 2003)		
ROSI (Cavusoglu/Mishra/Raghunathan, 2004; Tsiakis/Stephanides, 2005; Veiga/Eloff, 2007; Merete Hagen/ Albrechtsen/Hovden, 2008; Tashi/Ghernaouti-Hélie, 2008; Coronado et al., 2009; Dzazali/Sulaiman/Zolait, 2009; Pudar/Manimaran/Liu, 2009; Hayden, 2010; Leon/Saxena, 2010; Chai/Kim/Rao, 2011; Goldstein/ Chernobai/Benaroch, 2011; Fenz et al., 2013; Hua/ Bapna, 2013; Wang/Kannan/Ulmer, 2013; Gao/Zhong, 2015; Lowry/Moody, 2015; Nazareth/Choi, 2015; Posey/Roberts/Lowry, 2015; Alavi/Islam/Mouratidis, 2016; Muthukrishnan/Palaniappan, 2016; Young et al., 2016)		

human resources (Kankanhalli et al., 2003; Dhillon/Torkzadeh, 2006; Willison/Backhouse, 2006; Savola, 2007; Veiga/Eloff, 2007; Kraemer/Carayon/Clem, 2009; Atoum/Otoom/Abu Ali, 2014; Mijnhardt/Baars/Spruit, 2016; Soomro/Shah/Ahmed, 2016)	human resources	
financial resources (Kankanhalli et al., 2003; Sowa/Gabriel, 2009; Tu/Yuan, 2014; Muthukrishnan/Palaniappan, 2016)	financial resources	
cost control (Anderson/Moore, 2006)		
financial aspect (Ernest Chang/Ho, 2006; Dogaheh, 2010)		
security budget (Willison/Backhouse, 2006; Johnson/Goetz, 2007; NIST, 2008; Kraemer/Carayon/Clem, 2009; Lee/Larsen, 2009; Beresnevichiene/Pym/Shiu, 2010; Smith et al., 2010; Montesdioca/Maçada, 2015; Alavi/Islam/Mouratidis, 2016; Horne/Maynard/Ahmad, 2017)		
resource support (Vaughn/Henning/Siraj, 2003; Ransbotham/Mitra, 2009; Sowa/Gabriel, 2009; Abu-Musa, 2010; Wilkin/Chenhall, 2010; Zalewski et al., 2014; AlHogail, 2015)	resource strategy	
economic factors (Coronado et al., 2009; Sunyaev et al., 2009; Verendel, 2009; Fenz et al., 2013; Hua/Bapna, 2013; Horne/Maynard/Ahmad, 2017)		
resource strategy and value delivery (Yaokumah, 2014)		

Table 13: *Resources*

Appendix C: P5 - Definition of Metrics

Question	Metric	Metric with base set	Note
Are security patches up to date?	% available patches applied	Systems with all available patches applied	
	Σ security evaluation deficiency	Systems with security evaluation deficiencies	
	Σ blacklisted software	Systems with blacklisted software	Derived from workshop
Are all infrastructure components known?	Σ known systems	Systems which are known	Same as “infrastructure” but with an other base set
Are all published vulnerabilities of the infrastructure known?	Σ known vulnerabilities	Systems with vulnerabilities	
	Average vulnerabilities per system	-	Same as before
	% systems without severe vulnerabilities	-	Opposite and subset of the metric before
	% secured areas	Systems within a secured area	Moved from vulnerability - tested systems
	Vulnerability exposure	Systems with exposed vulnerabilities	Moved from vulnerability - patched systems
Are all systems scanned for vulnerabilities?	% tested and assessed systems	Systems tested/assessed	
	% whitstand targeted pentest	System withstand targeted pentest	

Table 14: *Minimize vulnerabilities*

Question	Metric	Metric with base set	Note
Are projects in time?	Ø project delays	Tasks with time delay	
Is budget enouth and effectively used?	ROSI	Tasks with positive ROSI	
	Security investment benefit	-	Same as ROSI
	Cost-benefit	-	Same as ROSI

	Information security budget	Tasks with enough budget	
	Cost and effort of patch process	-	Subset of task and ROSI
	% budget devoted to IS	-	Same as task budget
Is there enough qualified staff?	% qualified IS staff	Tasks with qualified staff	
	% responsibility sharing	Tasks with shared responsibilities	
	% in-house specialized staff dedicated to assessment of info-sec activities	Tasks with in-house specialized staff	

Table 15: *Optimize resources*

Question	**Metric**	**Metric with base set**	**Note**
Are all users known?	Σ users	Persons within the organization	
	% individuals screened	Persons which are screened	
Are departments involved in information security issues?	% departments represented in security committee	Persons represented in the security committee	
Are employees trained and aware?	% accounts compliant	-	Same as access control
	Σ security practice incentives	Persons got security incentives	
	Σ incidents reported by employees	Persons reported incidents	
	Ø training hours received	Persons received security training per time frame	
	% satisfactory accomplishment per training activity	Persons passed security training	
	Degree of awareness	-	Same as before
	% security budget spend on training	-	Same as budget and a subset of task
	Degree of organizational climate satisfaction (survey)	Persons with organizational climate satisfaction	
	Σ users briefed	Persons which receive briefing	

	Σ managers with NDA	Persons which are managers signed NDA	
	Employees dedicated to information security	-	Same as resources
	% Managers with information security certification	Persons which are managers which hold a IS certificate	
	Σ persons with security training	-	Same as before
Do employees violate against awareness policies?	Σ admin violations	Persons which are admins which violate against rules	
	Σ unauthorized website access	Persons which accessed websites unauthorized	
	Σ reasons for revocation	-	A base set connection is not possible
	Ø user population revoked	Persons with revoked rights	
	Σ personnel reprimanded or fired for security decisions/actions	Persons reprimanded for security reasons	If a person is fired, this person is out of scope

Table 16: *Maximize awareness*

Question	Metric	Metric with base set	Note
Are user accounts compliant?	% user accounts in compliance	System identities in compliance with rules	
	-	System identities linked to real persons	From workshop
	-	System identities with checked rights for linked persons	From workshop
Which users have admin rights?	Σ user with admin passwords	-	Same as checked with admin rights
	Σ superuser and root privileges	-	Same as before
How strong is the access protected?	Σ unauthorized access/intrusion success	System identities used for unauthorized access	

	Σ strong credential keys	-	Same as passwords which meet requirements
	Σ failed logon attempts	System identities with failed logon attempts	
	Σ logon violations	-	Same as before
	Σ password crack time	System identities with crack time under threshold	
	Σ attempts to change security settings	-	Not connected to base set
	% passwords meet minimum requirements	System identities with minimum password requirements	
	% two factor authentication	System identities with two factor authentication	

Table 17: *Maximize restrictions to resources*

Question	**Metric**	**Metric with base set**	**Note**
Are critical components physically protected?	Host criticality	Physical devices with critical business function	
	% critical equipment with adequate physical protection	Physical devices with adequate physical protection	

Table 18: *Maximize physical access restrictions*

Question	**Metric**	**Metric with base set**	**Note**
Are all infrastructure components known?	Σ systems	All infrastructure components	
	Σ critical assets	-	Subset of infrastructure components
	Σ critical areas	-	Subset of infrastructure components
	% asset visibility	Infrastructure components known	
Are all components configured according to the definition?	Σ configuration weaknesses	Infrastructure components with configuration weaknesses	

	% secured configurations	-	Same as before
	Σ security evaluation deficiency	-	Same as vulnerability
	Σ misconfigured devices	Infrastructure components with misconfigurations	
	Σ firewall devices with retrieved configurations	-	Subset of infrastructure component
	% system interfaces accepts only valid input	Infrastructure components which only accepts valid input on each interface	
	Σ systems certified	Infrastructure components certified	
Are versions up to date?	% available patches applied	-	Same as vulnerabilities
	Σ devices requiring remediation	Infrastructure components requiring remediation	
	% hosts require remediation	-	Same as before
Are communication channels known?	Σ external communication channels	Infrastructure components with communication channels that are externally visible	
	Σ remote access and wireless devices	Infrastructure components with remote access and wireless access	
	Σ access points	-	Same as before
Are all components protected against known attacks?	Σ detection mechanisms deficiency	Infrastructure components with no detection mechanism	
	Σ pc with antivirus	Infrastructure components with antivirus installed	
	Σ server with antivirus	-	Same as before
Are all components owned and monitored?	% information systems assets with owners	Infrastructure components with owner	
	% log files monitored	Infrastructure components with monitored log files	

Table 19: *Maximize infrastructure hardening*

Question	**Metric**	**Metric with base set**	**Note**
Are there vulnerabilities?	See other areas	Assets with vulnerabilities or weaknesses	
Are exploits or threats available?	Ø CVSS score	Assets with CVSS score above threshold	
	Σ identified potential threats	Assets with identified potential threats	
Are all components of the infrastructure related to a risk?	Ø computer/host criticality	Assets with criticality	
	% software and hardware classified	-	Same as before
	% assets with completed risk assessment	Assets with completed risk assessment	
	% risk assessment automatization	-	Not connected to base set
What is the probability?	% probability of compromise	Assets with probability over a threshold	
	Ø attack graph depth	Asset with attack graph depth over a threshold	
	Σ attack surface	-	Same as vulnerability
What is the impact in case of occurrence?	Σ worst case loss	Assets with worst case loss over threshold	
	Σ business value	-	Same as before
What is the current risk level?	Σ value at risk	-	Would be the key indicator
	Ø level of risk by area	-	Subset of level of risk
	Risk level	-	Same as before
	downstream risk	-	Not connected to base set
	it risk	-	Subset of risk
What is the accepted risk level?	Risk acceptance level	thresholds	These are the thresholds of the individual organization
	Σ risks accepted	Assets with accepted risks	
	Σ high risks accepted	-	Subset of accepted risks

Table 20: *Mitigate risk level*

Question	Metric	Metric with base set	Note
Are backups for components in place?	Σ remaining storage capacity	Assets with remaining storage capacity	
	Σ data recovery testing	Assets with tested data recovery	
	Σ protected files	Assets with all files protected	
Is it possible to recover a malfunction service?	Ø mean-time-to-repair	Assets with repair test	
	Business critical data recovery time	-	Same as before
	Critical data recording date	Assets with data recording date under threshold	
Do activities impact continuity?	Patch risk	Assets with patch risk over threshold	
	Ø mean-time-to-failure	Assets with m-t-t-f over threshold	
	Σ remaining storage capacity	-	Same as before
	Σ point solutions	Assets with point solutions	

Table 21: *Maximize continuity*

Question	Metric	Metric with base set	Note
Are all documented components available?	Ø service availability time	Assets with availability time under threshold	
	% network reachability	-	Same as before
	% systems reachability	-	Same as before
Are communication paths encrypted?	Σ unauthorized information disclosure	Assets with unauthorized information disclosure	
	% encrypted communications	Assets with encrypted communication paths	
	% media passes sanitization procedures	Assets which communicate over sanitization procedures	

Table 22: *Ensure CIA*

Question	Metric	Metric with base set	Note
Are policies in place?	Σ security policies	Rules	

	Policies in design phase	-	Subset of before
Are there policy violations?	% user accounts in compliance	-	Same as awareness
	Maturity level of current controls	Rules with maturity level under threshold	
	% penalties imposed to users	Rules with imposed penalties	
	Σ policy violations	Rules with violations	
Are policies accepted by the management?	% policies documented and approved	Rules documented and approved	
	% managers involved in the IS policy definition / evaluation / review	Rules with involved managers	
Are all rules fulfilled?	% compliance	-	Opposite of rules with violations
	Σ systems certified	-	Same as infrastructure
	Σ audits to the information security by outsourced firms	Rules audited by external organizations	
	% fulfilled regulations	-	Subset of rules
	% security requirements addressed in third party agreements	Rules addressed in third party agreements	

Table 23: *Maximize rule conformation*

Appendix D: Published Version of Publications

Prerequisite to Measure Information Security
A State of the Art Literature Review

Rainer Diesch[1,2], Matthias Pfaff[1,2] and Helmut Krcmar[2]
[1] *fortiss GmbH, An-Institut der Technischen Universität München, Guerickestr. 25, 80805 München, Germany*
[2] *Chair of Information Systems, Technischen Universität München, Boltzmannstr. 3, München, Germany*

Keywords: Security Measurement, Security Metrics, Cyber Security, Information Security, Literature Review.

Abstract: The field of information security is growing in research and practice over the past years. Recent studies highlight a gap in measuring and monitoring information security. In this context various definitions and synonymous expressions exist to describe information security. The aim of the work is to compare and delimit the various terms in this field of research and give a thematic overview of current articles in place. In particular, five dimensions of information security are developed and outlined. Additionally, an overview of possible research directions in the field of measuring and monitoring information security is provided.

1 INTRODUCTION

The interest in aspects of information security has increased significantly in recent years. There are technical, behavioral, managerial, philosophical and organizational aspects which address the protection of assets and mitigation of threats (Crossler et al., 2013). These aspects are not to be ignored for organizations since these can lead to great harm in case of disregard. (Frizell, 2015) reported a damage of $15m within one-quarter for Sony Pictures because of a security breach. This cost only included the direct costs of cleaning up the systems. The damage caused by the loss of reputation and other factors were not included. In 2016, the ransomware 'wannacry' infected thousands of computers in more than 150 countries. The damage was not only economically as people like patients were affected as their appointments were canceled based on system errors (Bentkower, 2017). Organizations are not just affected because of potential economic damage but also of legal requirements like the security-law in Germany (Bundesanzeiger, 2015).

Recent literature reviews on information security pointed out the need for intensified research in measuring and monitoring information security related data (D'Arcy and Herath, 2011; Crossler et al., 2013; Fenz et al., 2014; Sommestad et al., 2014). This is an obligatory aspect of information security management for making good decisions (Bayuk, 2013). Also, accurate models of the security problem are not in place (D'Arcy and Herath, 2011). A problem which causes a lack of measurement of information security aspects is that the identification of security related data is not well-known (Fenz et al., 2014). But a requirement to collect and measure security related data is to understand the success factors of information security (Sommestad et al., 2014).

The aim of this work is to gain an overview of current research in the field of measuring information security. A state-of-the-art literature analysis is carried out to obtain a comprehensive overview of the area. The goal is not just to show the literature but also to define the different terms in place. Since the understanding is a requirement for measurement, a definition becomes indispensable. Thematic classes of the research area are needed to observe and assign future research.

The paper is organized as follows: Section 2 outlines the used method with the scope and the search process to collect relevant literature. Section 3 consists of a descriptive analysis, the extracted definitions and thematic classification of the investigated literature. Part 4 shows current research challenges for each of the classes. Finally, this work concludes with a conclusion and limitation section.

2 METHOD

To provide a comprehensible literature review, the method of (Webster and Watson, 2002) and the tool-

Diesch, R., Pfaff, M. and Krcmar, H.
Prerequisite to Measure Information Security - A State of the Art Literature Review.
DOI: 10.5220/0006545602070215
In *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP 2018)*, pages 207-215
ISBN: 978-989-758-282-0

Table 1: Search process matrix.

Group	Resource	Hits[KW]	Hits[TA]	Relevant
Information Security	Information Management and Computer Security	99	7	7
	IEEE Transactions on Dependable and Secure Computing	8	1	1
	IEEE Transactions on Information Forensics and Security	7	0	0
	Computers & Security	84	12	9
Databases	Google Scholar	100	11	9
	ScienceDirect	41	6	4
	OpacPlus	110	17	11
Backward			10	10
Forward			24	19
Total		449	88	70

set of (vom Brocke et al., 2009) was used. The specific goals of this review are as follows:

1. Identify, define and delimit different terms in the field of information security.
2. Assign the relevant literature to the definitions and compare it with the used terms of the literature itself.
3. Thematic classification of the literature and show current research gaps.

Search Process: Initially, a keyword search is performed within peer-reviewed journals to select high quality articles. Journals from the security field were selected within the Scimago Journal & Country Rank (SJR) with the condition that they are part of the categories security, safety, risk or reliability. Two journals are added because they were used often in the basis literature reviews of (D'Arcy and Herath, 2011; Crossler et al., 2013; Fenz et al., 2014; Sommestad et al., 2014). These are 'Computers & Security' and 'Information Management & Computer Security'. To provide most of the relevant literature the databases ScienceDirect, OpacPlus and Google Scholar were added to the search. As the most relevant literature can be found within the first 100 result of Google Scholar the search was limited to these result set (Silic and Back, 2014). To limit the results the following keyword-string were used.

```
(it OR information OR cyber)
AND (resilience OR security)
AND (factors OR kpi OR measures OR metrics
OR measurement OR indicator OR management)
```

The first iteration of the search process resulted in a number of hits (Hits[KW]) which are shown in Table 1. After that, technical articles and those which are not related to the search topic were excluded based on their title and abstract (Hits[TA]). Finally, articles which described metrics or success factors of information security were marked as relevant. After that, a forward and backward search was carried out to get results which are relevant and were not yet found. The backward search contained all articles which were referenced in the previous iteration and which are of relevance for the information security measurement topic. Google Scholar (scholar.google.de) was used with its function 'Cited by' in order to identify all articles which reference the selected one.

3 FINDINGS

First, a descriptive statistic was done to get a background of the research area. The last row of table 1 shows the total amount of articles found in the literature. Only 15.59% of the original articles out of the first search round could be marked as relevant. This leads to the assumption that there are many different phenomena described in the research area. The high amount of articles also assumes the importance and presence in research. Many articles were identified in the forward and backward search (29) within conferences. This can be seen as an indication that the topic is still at the beginning of research. Technically oriented journals just show up with one relevant article. The quantification of information security is therefore mainly part of the security management or related area and not technical-driven.

Since there are many definitions and terms of information security in the literature, the next subsection compares and delimits them. Finally, a classification of the relevant literature in thematic classes are developed to better track and monitor future research.

3.1 The Terms in Information Security

A lot of different terms which describe 'information security' are in place during the review. These are 'Information Systems Security', 'IT Security', 'Information Security', 'Cyber Security' and 'Cyber Resilience'.

The basis of the delimitation in this article is the work of (von Solms and van Niekerk, 2013). They defined three terms in the security area. 'Information Security' (IS), 'Information and Communication Technology Security' (ICT) and 'Cyber Security' (CS). The delimitation of the terms is based on the assets which are protected. In this case, ICT is the protection of information which is stored or transmitted via a technical system. 'IT Security' or 'Systems Security' are defined as synonyms to ICT. IS differs from this because it is the protection of information which can be stored or transmitted without using technical systems. ICT is a part of IS because IS includes the protection of the underlying technology. CS now describes the protection of assets without any information but with a relationship to them. A bugging operation is an example of this. A technical system (phone) was attacked which has 'access' to information which is in human heads. CS is protecting technical systems which have or have no information stored and therefore also includes ICT. 'Cyber Resilience' (CR) firstly appears 2013 in form of resilience management (Crossler et al., 2013). The only attempt to define CR was done by (Björck et al., 2015). They showed 5 dimensions to differ CR from CS. One of these is assets. CR is not just about the protection of assets but also to ensure business delivery despite adverse cyber events. The correlation between the terms is shown in Figure 1.

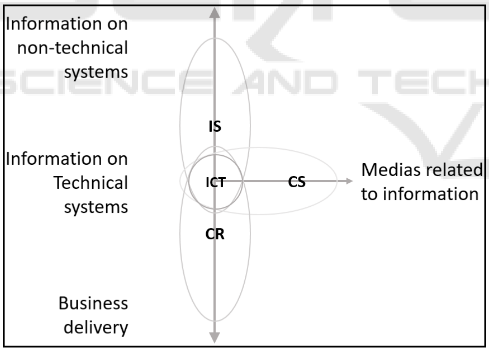
Information on non-technical systems
IS
Information on Technical systems
ICT
CS
Medias related to information
CR
Business delivery

Figure 1: Delimitation of terms.

According to the definition of ICT, IS, CS and CR, the literature was assigned respectively one or more of these in two iterations. First, the article was assigned the term, which the author had intended for this. The basis of the assignment was the terms of the title, abstracts and the keywords. Second, the articles were assigned the terms according to the definition above. This is done based on the context.

The result of the assignment shows that 23 out of 70 articles (32.86%) have the same assignment to the terms for both iterations. It is noticeable that the terms are often used as synonyms. Mainly IS is used as a synonym for ICT. Articles that use the term IS (60) often have just content of ICT included in the text (37) and not IS as defined. All authors used CS and CR as synonyms for ICT. The articles which describe CS or CR used the term IS instead of them. In the present literature, there are clear definitions of the terms, but the terms are not used based on them.

3.2 Thematic Classification

The relevant literature of this review is about measurement and metrics of ICT, IS, CS and CR. To observe papers in future and better understand the context, there are several classes produced in this literature review which are based on the keywords of the underlying articles. Each paper is assigned to one of the classes which are shown in Table 2.

3.2.1 Security Management

'Information security management' is used to describe activities for the protection of valuable information assets and mitigate various risks to information coming from all aspects of the organizations environment by applying the security technology and management process (Ernest Chang and Ho, 2006). In other words, it is about processes to control, classify and manage information as well as different guidelines and policies therefrom.

Organization and Governance: These articles deal with organizational processes, policies and their effectiveness. A subset of articles also provides information and simulations of security investments and the security economy within organizations. There are also frameworks on how to set up a secure environment with a culture and guides to good policies included.

Awareness: The role of human in information security is a substantial stream in research (Kraemer et al., 2009). Therefore organizations have to consider dealing with security awareness.

Evaluation: These articles deal with the question of which success factors lead to good management or which factors influence the success of implementing a security management system. Another aspect is the validation and verification of policies and factors which causes better ones.

3.2.2 Security Measurement

Security metrics refer to the interpretation of measurements of the security performance, level and indicators (Savola and Heinonen, 2011). Therefore

Table 2: Thematic classification of the literature.

Security management	Organization and Governance	(Geer et al., 2003; Hong et al., 2003; Trèek, 2003; von Solms and von Solms, 2004; Gupta and Hammond, 2005; Anderson and Moore, 2006; Ernest Chang and Ho, 2006; Johnson and Goetz, 2007; Veiga and Eloff, 2007; Atoum et al., 2014; Narain Singh et al., 2014; Yaokumah, 2014; Fenz et al., 2014; AlHogail, 2015; Horne et al., 2017)
	Awareness	(Straub and Welke, 1998; Velki et al., 2014; Tran et al., 2016)
	Evaluation	(von Solms et al., 1994; Kraemer et al., 2009; Abu-Musa, 2010; Hall et al., 2011; Norman and Yasin, 2012; Tu and Yuan, 2014; Alqahtani, 2015; Muthukrishnan and Palaniappan, 2016; Azuwa et al., 2017)
Security measurement	Development	(Wang and Wulf, 1997; Sharman et al., 2004; Herrera, 2005; Tanna et al., 2005; Tashi and Ghernaouti-Hélie, 2008; Sowa and Gabriel, 2009; Leon and Saxena, 2010; LeMay et al., 2011; Idika and Bhargava, 2012; Jones and Horowitz, 2012; Tariq, 2012; Bayuk and Mostashari, 2013; Zalewski et al., 2014; Mazur et al., 2015; Collier et al., 2016; Young et al., 2016)
	Taxonomy	(Vaughn et al., 2003; Savola, 2007; Savola, 2009; Verendel, 2009; Purboyo et al., 2011; Pendleton et al., 2017)
	Security Metrics	(Boyer and McQueen, 2007; Premaratne et al., 2008; Dogaheh, 2010; Jafari et al., 2010; Mermigas et al., 2013; Holm and Afridi, 2015)
	Effectiveness	(Coronado et al., 2009; Bayuk, 2013; Savola, 2013)
	Visualization	(Savola and Heinonen, 2011)
Human Behavior		(Gonzalez and Sawicka, 2002; Ifinedo, 2012; Crossler et al., 2013; Vance et al., 2014; Montesdioca and Maçada, 2015; Alavi et al., 2016)
Practical Frameworks		(IT Governance Institute, 2007; NIST, S. P., 2008; ISO/IEC, 2009; Hayden, 2010; CCIB, 2017)

measurement is the process of estimating attributes of an object while metrics refer to assign a value to an object (Pendleton et al., 2017).

Development: There are methods to develop metrics for information security aspects. Examples of them are metrics which are developed based on different approaches like Goal-Question-Metric (Savola, 2007; Bayuk, 2013) or attack-graphs (Premaratne et al., 2008; LeMay et al., 2011; Idika and Bhargava, 2012). There are also frameworks with descriptions of good metrics and how to implement them.

Taxonomy: The taxonomies in this class describe and characterize different measurement approaches and several classes of metrics which are based on the objective and the measurement goal.

Security Metrics: A security metric is a quantitative indicator for various targets in operational security (Verendel, 2009). The articles focus on specific metrics and evaluate or simulate them.

Effectiveness: The effectiveness of metrics to measure information security is discussed here. The articles compare different frameworks to generate measurements and discuss different metrics in detail.

Visualization: The management has the requirement to easily understand and therefore react very fast to changed metrics (Jafari et al., 2010; Savola and Heinonen, 2011). Therefore these articles deal with an optimal visualization of complex metrics.

3.2.3 Human Behavior

Human behavior or human factors affecting information security are not to be confused with the awareness described above. These articles deal with different behavior theories like 'protection motivation' or 'planned behavior'. The perspective of attackers is included in form of social engineering attacks and factors which can prevent them.

3.2.4 Practical Frameworks

Frameworks from practice which also called best-practices are included. They are developed for practitioners to deal with information security management systems or security effectiveness.

4 DISCUSSION

The quantitative analysis of the relevant literature revealed that under the subject of the measurement of information security many phenomena can be interpreted. An exact delimitation of the topic area from others, such as management processes, would be helpful for tracking this issue. In the case of the definitions, it can be argued that there is less research in CS and CR available than in ICT and IS. Context is the measurement of information security. Future research should pay attention to the correct and uniform use of the concepts and develop them further. The thematic classification shows potential research areas in each of the different classes. The following part describes these research areas within the different classes based on the given literature:

Security Management: To fundamentally make decisions in the area of systems security it is necessary to know the current information security status within an organization and know the weaknesses and where they are. This is currently still a gap in research (von Solms et al., 1994; Johnson and Goetz, 2007; Tu and Yuan, 2014; Horne et al., 2017). (Mermigas et al., 2013) goes one step further and says that organizations need to know how secure they are at any given point in time. A requirement to do this is the understanding of the success factors of information security within organizations and how they are related (Kraemer et al., 2009; Norman and Yasin, 2012; Horne et al., 2017). If the security status can be operationalized it is also possible to measure if the security program as well as their countermeasures or policies of the organization are effective or not. This is also an undeveloped research task (Gupta and Hammond, 2005; Fenz et al., 2014; Atoum et al., 2014). The present literature review excludes those articles which did not contain any security success factors. Further work could show and categorize the existing direct and indirect success factors which are already in place. This could be the basis for an empirical evaluation and a better understanding of security in organizations.

Security Measurement: The measurement of security as a property and the development of security metrics itself are in a very early research stage and quite underdeveloped (Savola, 2009; Savola and Heinonen, 2011; Zalewski et al., 2014). Knowing how to measure the security as well as the defense level of organizations and generally of systems is a gap in research (Vaughn et al., 2003; Purboyo et al., 2011; Alavi et al., 2016). The area of measurement goes also a step back and asks for practices to measure the coverage of visibility. This is about effective and adequate assessments of risks and assets and how it can be monitored (Abu-Musa, 2010). Specifically, there is a gap in explored metrics for the measurement of information security, which are associated with existing models and thus provide the basis for cross-sectoral and organizational independent security comparison (Sowa and Gabriel, 2009; Bayuk and Mostashari, 2013). It is often the case that just the security management program is measured and not the security itself (Tashi and Ghernaouti-Hélie, 2008; Jafari et al., 2010). There is not just a gap in developing and creating concrete metrics but also in tools to gather information security related data and monitor the security status (Wang and Wulf, 1997; Boyer and McQueen, 2007; Crossler et al., 2013). Based on this work, current metrics in place could be shown and linked to the frameworks, success factors and development models.

Human Behavior: Human behavior is little represented in this review. In case of measurement there is an open question on how to capture actual behavior (Crossler et al., 2013).

Practical Frameworks: Practical frameworks are designed to help organizations to implement and use security related information in management. The only framework who describes metrics to monitor the security status says that these metrics are not covering the minimum security requirements (NIST, S. P., 2008). Also, the automatic way to collect and measure the data is a requirement for good and repeatable metrics (NIST, S. P., 2008). Other frameworks like (IT Governance Institute, 2007; ISO/IEC, 2009) addresses just the effectiveness of security management processes and not the security status of the assets and environment itself. An empirical evaluation or test of the described issues is not present literature.

5 CONCLUSION

There is a gap in measuring and monitoring information security in current research (D'Arcy and Herath, 2011; Crossler et al., 2013; Fenz et al., 2014; Sommestad et al., 2014). To develop a measurement and collect information security related data, it is necessary to understand information security and the success factors influencing it (Sommestad et al., 2014).

This literature review after (Webster and Watson, 2002; vom Brocke et al., 2009) included journals of the information security area as well as databases. The search process results in the identification of 70 articles which are interesting for measuring information security. The chronological analysis shows that the topic has become more and more important in the past years. Also, there are a lot of terms in place which are used in different contexts. This becomes clear as soon as the keywords, the title and the contents of the articles are compared with respect to the term. The delimitation of the terms is based on the work of (von Solms and van Niekerk, 2013) and is extended in this review based on the definitions of (Björck et al., 2015) to get an overview of the current terms and their usage. Past literature uses the terms as synonyms which should be avoided in the future.

The thematic classification of the literature can help to capture future research and better assign them a context. It is shown that the measurement of information security is often a management topic. This is useful because the measurement allows an objective control and a well-based decision-making in connection to information security.

The relevant articles show that information security is necessary for organizations and decision-makers. To manage, make good decisions and capture the current state of information security, a measurement is needed (Bayuk, 2013). Current research does not adequately cover this topic. Future research should investigate in the definition of success factors for information security to fulfill the requirement of understanding security success factors (Kraemer et al., 2009; Norman and Yasin, 2012; Horne et al., 2017) and define a current state of security (von Solms et al., 1994; Johnson and Goetz, 2007; Mermigas et al., 2013; Tu and Yuan, 2014; Horne et al., 2017). Therefore concrete metrics and tools to monitor these need to be developed (Wang and Wulf, 1997; Vaughn et al., 2003; Boyer and McQueen, 2007; Sowa and Gabriel, 2009; Purboyo et al., 2011; Crossler et al., 2013; Bayuk and Mostashari, 2013; Alavi et al., 2016). Future research could then evaluate the effectiveness of security programs and actions based on the security quantification (Gupta and Hammond, 2005; Fenz et al., 2014; Atoum et al., 2014).

6 LIMITATIONS

The limitations are based on the search process. The initial search was performed based on highly ranked journals. Therefore it is possible that articles within conferences or not included journals could influence the results of this literature review. The same could apply for articles which are excluded based on their title and abstract. It cannot be ruled out that relevant articles have been removed which does not outline to the search topic but has relevant content. In order to limit these shortcomings, the database search, as well as the forward and backward search, was performed. Moreover, this literature review does not cover management or interdisciplinary journals which could also be interesting for measuring security.

REFERENCES

Abu-Musa, A. (2010). Information security governance in saudi organizations: An empirical study. *Information Management & Computer Security*, 18(4):226–276.

Alavi, R., Islam, S., and Mouratidis, H. (2016). An information security risk-driven investment model for analysing human factors. *Information and Computer Security*, 24(2):205–227.

AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior*, 49:567–575.

Alqahtani, A. (2015). Towards a framework for the potential cyber-terrorist threat to critical national infrastructure. *Information and Computer Security*, 23(5):532–569.

Anderson, R. and Moore, T. (2006). The economics of information security. *Science (New York, N.Y.)*, 314:610–613.

Atoum, I., Otoom, A., and Abu Ali, A. (2014). A holistic cyber security implementation framework. *Information Management & Computer Security*, 22(3):251–264.

Azuwa, M. P., Sahib, S., and Shamsuddin, S. (2017). Technical security metrics model in compliance with iso/iec 27001 standard. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, 1(4):280–288.

Bayuk, J. and Mostashari, A. (2013). Measuring systems security. *Systems Engineering*, 16(1):1–14.

Bayuk, J. L. (2013). Security as a theoretical attribute construct. *Computers & Security*, 37:155–175.

Bentkower, M. (2017). Assessing the real damage of the 'wannacry' malware attack.

Björck, F., Henkel, M., Stirna, J., and Zdravkovic, J. (2015). Cyber resilience – fundamentals for a definition. In *New Contributions in Information Systems and Technologies*, Advances in Intelligent Systems and Computing, pages 311–316. Springer International Publishing, Cham.

Boyer, W. and McQueen, M. (2007). Ideal based cyber security technical metrics for control systems. In *Critical information infrastructures security*, pages 246–260.

Bundesanzeiger (2015). Gesetz zur erhoehung der sicherheit informationstechnischer systeme (it-sicherheitsgesetz). *Bundesgesetzblatt*, 1(31):1324–1331.

CCIB (2017). *Common Criteria for Information Technology Security Evaluation: Part 2: Security functional components, Version 3.1, Revision 5.* Common Criteria.

Collier, Z. A., Panwar, M., Ganin, A. A., Kott, A., and Linkov, I. (2016). Security metrics in industrial control systems. In Colbert, E. J. M. and Kott, A., editors, *Cyber-security of SCADA and other industrial control systems*, Advances in Information Security, pages 167–185. Springer, Switzerland.

Coronado, A. S., Mahmood, M. A., Pahnila, S., and Luciano, E. M. (2009). Measuring effectiveness of information systems security: An empirical research. In *15th Americas Conference on Information Systems*.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., and Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, 32:90–101.

D'Arcy, J. and Herath, T. (2011). A review and analysis of deterrence theory in the is security literature: Making sense of the disparate findings. *European Journal of Information Systems*, 20(6):643–658.

Dogaheh, M. A. (2010). Introducing a framework for security measurements. In *IEEE International Conference on Information Theory and Information Security*, pages 638–641.

Ernest Chang, S. and Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems*, 106(3):345–361.

Fenz, S., Heurix, J., Neubauer, T., and Pechstein, F. (2014). Current challenges in information security risk management. *Information Management & Computer Security*, 22(5):410–430.

Frizell, S. (2015). Sony the interview hack: Studio spending $15 million to deal with it.

Geer, D., Hoo, K. S., and Jaquith, A. (2003). Information security: Why the future belongs to the quants. *IEEE Security & Privacy Magazine*, 1(4):24–32.

Gonzalez, J. J. and Sawicka, A. (2002). A framework for human factors in information security. In *2002 WSEAS International Conference on Information Security, Hardware/Software Codesign, E-Commerce and Computer Networks*, pages 1871–1877.

Gupta, A. and Hammond, R. (2005). Information systems security issues and decisions for small businesses. *Information Management & Computer Security*, 13(4):297–310.

Hall, J. H., Sarkani, S., and Mazzuchi, T. A. (2011). Impacts of organizational capabilities in information security. *Information Management & Computer Security*, 19(3):155–176.

Hayden, L. (2010). *IT security metrics: A practical framework for measuring security & protecting data*. McGraw Hill, New York.

Herrera, S. (2005). Information security management metrics development. In *Proceedings / 39th Annual 2005 International Carnahan Conference on Security Technology*, pages 51–56.

Holm, H. and Afridi, K. K. (2015). An expert-based investigation of the common vulnerability scoring system. *Computers & Security*, 53:18–30.

Hong, K.-S., Chi, Y.-P., Chao, L. R., and Tang, J.-H. (2003). An integrated system theory of information security management. *Information Management & Computer Security*, 11(5):243–248.

Horne, C. A., Maynard, S. B., and Ahmad, A. (2017). Information security strategy in organisations: Review, discussion and future research. *Australasian Journal of Information Systems*, 21.

Idika, N. and Bhargava, B. (2012). Extending attack graph-based security metrics and aggregating their application. *IEEE Transactions on Dependable and Secure Computing*, 9(1):75–85.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 31(1):83–95.

ISO/IEC (2009). *ISO/IEC 27004:2009(E) - Information technology - Security techniques - Information security management - Measurement*. ISO/IEC.

IT Governance Institute (2007). *COBIT 4.1: Framework, control objectives, management guidelines, maturity models*. IT Governance Institute, Rolling Meadows.

Jafari, S., Mtenzi, F., Fitzpatrick, R., and O'Shea, B. (2010). Security metrics for e-healthcare information systems: A domain specific metrics approach. *International Journal of Digital Society (IJDS)*, 1(4):238–245.

Johnson, M. E. and Goetz, E. (2007). Embedding information security into the organization. *IEEE Security & Privacy Magazine*, 5(3):16–24.

Jones, R. A. and Horowitz, B. (2012). A system-aware cyber security architecture. *Systems Engineering*, 15(2):225–240.

Kraemer, S., Carayon, P., and Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & Security*, 28(7):509–520.

LeMay, E., Ford, M. D., Keefe, K., Sanders, W. H., and Muehrcke, C. (2011). Model-based security metrics using adversary view security evaluation (advise). In *Eighth International Conference on Quantitative Evaluation of SysTems*, pages 191–200.

Leon, P. G. and Saxena, A. (2010). An approach to quantitatively measure information security. In *3rd India Software Engineering Conference*.

Mazur, K., Ksiezopolski, B., and Kotulski, Z. (2015). The robust measurement method for security metrics generation. *The Computer Journal*, 58(10):2280–2296.

Mermigas, D., Patsakis, C., and Pirounias, S. (2013). Quantification of information systems security with stochastic calculus. In *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop*, pages 1–9.

Montesdioca, G. P. Z. and Maçada, A. C. G. (2015). Measuring user satisfaction with information security practices. *Computers & Security*, 48:267–280.

Muthukrishnan, S. M. and Palaniappan, S. (2016). Security metrics maturity model for operational security. In *IEEE Symposium on Computer Applications and Industrial Electronics*, pages 101–106.

Narain Singh, A., Gupta, M. P., and Ojha, A. (2014). Identifying factors of "organizational information security management". *Journal of Enterprise Information Management*, 27(5):644–667.

NIST, S. P. (2008). *800-55r1: Performance measurement guide for information security*. National Institute of Standards and Technology, Gaithersburg, MD.

Norman, A. A. and Yasin, N. M. (2012). Information systems security management (issm) success factor: Retrospection from the scholars. In *Proceedings of the 11th European Conference on Information warfare and security*.

Pendleton, M., Garcia-Lebron, R., Cho, J.-H., and Xu, S. (2017). A survey on systems security metrics. *ACM Computing Surveys*, 49(4):1–35.

Premaratne, U., Samarabandu, J., Sidhu, T., Beresh, B., and Tan, J.-C. (2008). Application of security metrics in auditing computer network security: A case study. In *4th International Conference on Information and Automation for Sustainability*, pages 200–205.

Purboyo, T. W., Rahardjo, B., and Kuspriyanto (2011). Security metrics: A brief survey. In *2011 2nd International Conference on Instrumentation, Communications, Information Technology and Biomedical Engineering*, pages 79–82.

Savola, R. (2007). Towards a security metrics taxonomy for the information and communication technology industry. In *International Conference on Software Engineering Advances (ICSEA)*, pages 60–66.

Savola, R. M. (2009). A security metrics taxonomization model for software-intensive systems. *Journal of Information Processing Systems*, 5(4):197–206.

Savola, R. M. (2013). Quality of security metrics and measurements. *Computers & Security*, 37:78–90.

Savola, R. M. and Heinonen, P. (2011). A visualization and modeling tool for security metrics and measurements management. In *2011 Information Security for South Africa*, pages 1–8.

Sharman, R., Rao, R., and Upadhyaya, S. (2004). Metrics for information security: A literature review. In *10th Americas Conference on Information Systems*.

Silic, M. and Back, A. (2014). Information security: Critical review and future directions for research. *Information Management & Computer Security*, 22(3):279–308.

Sommestad, T., Hallberg, J., Lundholm, K., and Bengtsson, J. (2014). Variables influencing information security policy compliance: A systematic review of quantitative studies. *Information Management & Computer Security*, 22(1):42–75.

Sowa, S. and Gabriel, R. (2009). Multidimensional management of information security: A metrics based approach merging business and information security topics. In *International Conference on Availability, Reliability and Security*, pages 750–755. IEEE.

Straub, D. W. and Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly*, 22(4):441.

Tanna, G. B., Gupta, M., Rao, H. R., and Upadhyaya, S. (2005). Information assurance metric development framework for electronic bill presentment and payment systems using transaction and workflow analysis. *Decision Support Systems*, 41(1):242–261.

Tariq, M. I. (2012). Towards information security metrics framework for cloud computing. *International Journal of Cloud Computing and Services Science (IJ-CLOSER)*, 1(4).

Tashi, I. and Ghernaouti-Hélie, S. (2008). Efficient security measurements and metrics for risk assessment. In *The Third International Conference on Internet Monitoring and Protection*, pages 131–138.

Tran, H., Campos-Nanez, E., Fomin, P., and Wasek, J. (2016). Cyber resilience recovery model to combat zero-day malware attacks. *Computers & Security*, 61:19–31.

Trèek, D. (2003). An integral framework for information systems security management. *Computers & Security*, 22(4):337–360.

Tu, Z. and Yuan, Y. (2014). Critical success factors analysis on effective information security management: A literature review. In *20th Americas Conference on Information Systems*.

Vance, A., Eargle, D., Anderson, B. B., and Kirwan, C. B. (2014). Using measures of risk perception to predict information security behavior: Insights from electroencephalography (eeg). *Journal of the Association for Information Systems*, 15:679–722.

Vaughn, R. B., Henning, R., and Siraj, A. (2003). Information assurance measures and metrics - state of practice and proposed taxonomy. In *Proceedings of the 36th Annual Hawaii International Conference on System Sciences*.

Veiga, A. D. and Eloff, J. H. P. (2007). An information security governance framework. *Information Systems Management*, 24(4):361–372.

Velki, T., Solic, K., and Ocevcic, H. (2014). Development of users' information security awareness questionnaire (uisaq) — ongoing work. In *37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pages 1417–1421.

Verendel, V. (2009). Quantified security is a weak hypothesis: A critical survey of results and assumptions. In *Proceedings of the 2009 workshop on New security paradigms workshop*.

vom Brocke, J., Simons, A., Niehaves, B., Riemer, K., Plattfaut, R., and Cleven, A. (2009). Reconstructing the giant: On the importance of rigour in documenting the literature search process. *17th European Conference on Information Systems (ECIS)*.

von Solms, B. and von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security*, 23(5):371–376.

von Solms, R., van der Haar, H., von Solms, S. H., and Caelli, W. J. (1994). A framework for information security evaluation. *Information & Management*, 26(3):143–153.

von Solms, R. and van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38:97–102.

Wang, C. and Wulf, W. A. (1997). Towards a framework for security measurement. In *20th National Information Systems Security Conference*, pages 522–533.

Webster, J. and Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, 26(2):xiii–xxiii.

Yaokumah, W. (2014). Information security governance implementation within ghanaian industry sectors. *Information Management & Computer Security*, 22(3):235–250.

Young, D., Lopez, J., Rice, M., Ramsey, B., and McTasney, R. (2016). A framework for incorporating insurance in critical infrastructure cyber risk strategies. *International Journal of Critical Infrastructure Protection*, 14:43–57.

Zalewski, J., Drager, S., McKeever, W., and Kornecki, A. J. (2014). Measuring security: A challenge for the generation. In *2014 Federated Conference on Computer Science and Information Systems*, Annals of Computer Science and Information Systems, pages 131–140.

Computers & Security 92 (2020) 101747

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

A comprehensive model of information security factors for decision-makers

Rainer Diesch[a,b,*], Matthias Pfaff[a,b], Helmut Krcmar[b]

[a] *fortiss GmbH, Guerickestr. 25, 80805 Munich, Germany*
[b] *Technical University of Munich, Boltzmannstr. 3, 85748 Garching, Germany*

ARTICLE INFO

Article history:
Received 9 January 2019
Revised 9 December 2019
Accepted 4 February 2020
Available online 4 February 2020

Keywords:
Key Security Indicators
Security Success
Security Model
Security Management Decision-Making
Expert Interview

ABSTRACT

Decision-making in the context of organizational information security is highly dependent on various information. For information security managers, not only relevant information has to be clarified but also their interdependencies have to be taken into account. Thus, the purpose of this research is to develop a comprehensive model of relevant management success factors (MSF) for organizational information security. First, a literature survey with an open-axial-selective analysis of 136 articles was performed to identify factors influencing information security. These factors were categorized into 12 areas: physical security, vulnerability, infrastructure, awareness, access control, risk, resources, organizational factors, CIA, continuity, security management, compliance & policy. Second, an interview series with 19 experts from the industry was used to evaluate the relevance of these factors in practice and explore interdependencies between them. Third, a comprehensive model was developed. The model shows that there are key-security-indicators, which directly impact the security-status of an organization while other indicators are only indirectly connected. Based on these results, information security managers should be aware of direct and indirect MSFs to make appropriate decisions.

1. Introduction

Today, most businesses are based or even fully dependent on information such as financial data for banks to stay at the market and be competitive (Knapp et al., 2006). According to thycotic, 62 % of all cyber-attacks are hitting small- and mid-sized businesses of which 60 % are going out of businesses six months after such an attack (Thycopic Software Ltd., 2017). 53 % of the attacks are causing $500.000 or more (Cisco Systems Inc., 2018) while the average cost of a data breach was $3.86 million (Ponemon Institute LLC, 2018). Not just financial losses are a risk but also legal and reputation repercussions (Tu and Yuan, 2014). Therefore, it is necessary for organizations to keep their information and the underlying technology secure against business-harming attacks.

In the past, information security was purely a technical concern and therefore, technical employees were responsible for information security issues within an organization (Willison and Backhouse, 2006). This perspective fails when it comes to a comprehensive and holistic view and the overall security strategy. Thus, in the past years, there was a shift from the executive technology expert to a management responsibility and a more business-focused view protecting information (Ashenden, 2008; Ransbotham and Mitra, 2009; Yeh and Chang, 2007). Nowadays, security managers are fully responsible to consider and respond to information security issues (Abu-Musa, 2010; Soomro et al., 2016). Various cases like the “Equifax breach” had shown the consequences for the top management in case of information security disregards. There, over 146 million personal information were stolen because of an unpatched system, which was a technical shortcoming. This causes, that the company gets rid of their CEO, CIO, and CSO by the “retirement” of them right after the breach (Bernard and Cowley, 2017). The technical personal was not affected. This goes further in manifesting the management responsibility within laws like the German Stock Corporation Act (§91 Section 2) which also requires an active risk management within companies.

Because of the shift from a technical to a management perspective, the research focus also changed from studies in a technical context to exploring the management role (Soomro et al., 2016). Managers must be able to take technical threats as well as other factors like human behavior into account to take the right and effective actions to mitigate threats (Coronado et al., 2009). To provide necessary funds, make good decisions and argue to the business, it is necessary for information security managers to

[*] Corresponding author at: Guerickestr. 25, 80805 Munich, Germany.
E-mail address: diesch@fortiss.org (R. Diesch).

https://doi.org/10.1016/j.cose.2020.101747

understand the complexity of information security (Willison and Backhouse, 2006) and have a comprehensive view on the topic (Soomro et al., 2016). This comprehensive view with specific factors and their interdependencies as well as the impact on the security status of an organization is still a gap in research (Diesch et al., 2018; Horne et al., 2017; Kraemer et al., 2009; Norman and Yasin, 2013; Soomro et al., 2016). Therefore, this study has the purpose to identify the key factors, evaluate them and explore interdependencies to finally generate a comprehensive model to understand the information security complexity and thus provide good information security management decisions.

The remaining research article is structured as follows. In Section 2, previous work on management practices and management success factors (MSF) in information security is described and the need for a comprehensive information security model with current shortcomings is shown. In Section 3, the three-step methodology which contains the literature survey, the literature analysis, and the expert interview series is presented. In Section 4, the evaluated MSFs are provided. The MSFs in conjunction with interdependencies are proposed as a comprehensive model in Section 5. In Section 6, a critical discussion of the results and areas for future research are highlighted. A conclusion is given in Section 7.

2. Background and motivation

This chapter is divided into three sections. In Section 2.1, standards and best practices in information security management for practitioners and their shortcomings are described. In Section 2.2, the term MSF and the current state of the art in research regarding this topic is introduced. In Section 2.3 the need for practitioners, as well as the gap in the literature, are highlighted to motivate this research.

2.1. Standards and best practices

Information security management is often build based on international standards or best practices (Hedström et al., 2011). The terms “standard” and “best practice” are often used as synonyms but “standards” are usually checked by an international standardization organization while “best practices” and other frameworks are published independently.

The most common standard from such an organization is the ISO/IEC 27000-series (ISO/IEC, 2018). This standard is widely accepted, play an important role and it is possible to certify the organizational information security based on it (Siponen and Willison, 2009). The ISO/IEC 27000-series defines basic requirements in order to implement an information security management system. Also, control guidance, implementation guidance, management measures, and the risk management approach is specified. Special sub-norms are also included in the series, for example, the ISO/IEC 27011 which deals especially with telecommunication organizations.

In addition to the information security management standard, there are frameworks or best practices like the NIST SP800-series (NIST, 2018b), the Standard of Good Practices from the Information Security Forum (ISF) (ISF, 2018) or the COBIT framework (ISACA, 2012). These best practices are used to implement an information security management system (ISMS), define and develop controls and address the most pressing problems regarding information security with an overview for their risk mitigation strategy (Mijnhardt et al., 2016). All in all, security standards provide a common basis for organizations to help reducing risks by developing, implementing and measuring security management (Ernest Chang and Ho, 2006).

Information security management certificates do provide a basic assurance level and show that some security measures are available. But in practice, experts are skeptical about certificates. Experts mentioned, that standards do help with compliance but not always help to reduce risk or improve security (Johnson and Goetz, 2007). Lee et al. (2016) show, that a higher security standard does not necessarily lead to a higher security level. The following shortcomings of standards were highlighted in the past literature:

(1) Well known standards are very generic in scope and tend to be very abstract (Siponen and Willison, 2009). For these standards, concrete countermeasures and combinations of them are missing, which leads to inefficient or even misleading risk mitigation strategies (Fenz et al., 2013).
(2) Standards consists of a huge amount of information. For example, the ISO 27000-series consists of 450 items with 9 focus areas. This complexity and the fact, that there are rarely fully implemented standards in small- and medium-sized businesses in place, leads to a fall back to ad-hoc implementations. An easy to understand toolkit is missing (Mijnhardt et al., 2016).
(3) The defined controls and countermeasures of the frameworks are often implemented without sufficient consideration of the daily work or their need (Hedström et al., 2011). This is because the organization usually do not consider the relationships between the security concepts (Fenz et al., 2013) and do not check whether a control is really necessary or less critical (Bayuk and Mostashari, 2013; Tu and Yuan, 2014).
(4) Rigorous empirical studies which consider different factors which may affect the decisions and validate the standards and best practices are missing in literature (Diesch et al., 2018; Siponen and Willison, 2009).
(5) There are regional differences in the use and contexts of frameworks. For example, the NIST SP800-series is “developed to address and support the security and privacy needs of U.S. Federal Government information and information systems” (NIST, 2018b) while the current standard in Australia is the IS0/IEC 27000-series (Smith et al., 2010). Therefore the NIST SP800 framework “is individually useful but (outside of the U.S.) do not provide a cohesive and explicit framework to manage information security” (Smith et al., 2010).

2.2. Information security success

Besides standards and best practices which were described before, there are theories and concepts in the literature which help decision-makers in information security. Managers need to know the current information security status of their organizational assets to make decisions. If there are not well protected, they need possible sets of controls with the consideration of the related costs to improve the information security situation (Diesch et al., 2018; Horne et al., 2017; Johnson and Goetz, 2007; Tu and Yuan, 2014; von Solms et al., 1994).

The literature deals with MSFs to describe the state of information security which is needed in practice. The term was used first in 1987 to describe factors which take into account as “catalysts to generate new and more effective systems security activities” in the security context (Wood, 1987). After that the theory of information systems success of DeLone and McLean (1992) deals with different dependent and independent variables, which are indicating a successful information systems strategy and that they can be categorized into dimensions. Recent studies used other terms in the context of information security:

1. “Information systems security management success factors” are factors to show the state of elements, which has to anticipate

preventing information security failure in the e-commerce context (Norman and Yasin, 2013).

2. "Critical success factors" describe factors, which influence the successful implementation of an information security management system (Tu and Yuan, 2014).
3. "Critical success factors are described as key areas in the firm that, if they are satisfactory, will assure successful performance for the organization" (Tu et al., 2018).

In this research, management success factors (MSF) are defined as factors to show the state of elements, which has to take into account in order to make appropriate management decisions in the information security context of an organization. If the security decisions are appropriate, it assures a successful security performance for the organization.

Current literature mostly looks on factors which influence security separately. To highlight just a view studies, they separately deal with organizational factors (Ernest Chang and Ho, 2006; Hall et al., 2011; Kankanhalli et al., 2003; Kraemer et al., 2009; Mijnhardt et al., 2016; Narain Singh et al., 2014), policy compliance issues (Boss et al., 2009; Goel and Chengalur-Smith, 2010; Höne and Eloff, 2002; Ifinedo, 2012; Johnston et al., 2016; Lowry and Moody, 2015a) or human factors (Alavi et al., 2016; AlHogail, 2015; Ashenden, 2008; Gonzalez and Sawicka, 2002; Kraemer et al., 2009). The reason for the separation is, that security is managed in a separate manner in different departments which includes information security, risk management, business continuity, operational security (Tashi and Ghernaouti-Hélie, 2008). This shows that various studies are available which do discuss different factors in great detail but do not include a integral view on them. There are just a view attempts to consolidate the body of knowledge in comprehensive MSFs. The information systems success theory explains six factors which are contributing to the systems success (DeLone and McLean, 1992). This view does not include specific security considerations including the costs and available countermeasures that a manager must consider. The authors self-criticized the proposed theory because of the missing evaluation. The only other success factor model was a model of factors, influencing the successful implementation of an information security management system (Norman and Yasin, 2013) and not the security decisions of managers itself.

2.3. Shortcomings in literature and practice

As the Sections 2.1 and 2.2 suggest, there are a view shortcomings in literature for supporting decisions on the security management level. A recent survey of McKinsey & Company with 1125 managers involved in 2017 identified three main problems, managers face in order to deal with information security issues (Boehm et al., 2017). These are *the lack of structure* within reports with dozens of indicators with inconsistent and too-high levels of details. The *lack of clarity* because of reports, which are too technical which a manager typically not understand. A *lack of consistent real-time data*.

The *lack of clarity* within reports is not just present in practice. Managers do not know all technical details and do not need them because of their teams and experts (Fenz et al., 2013; May, 1997). But they have to establish a security establishment and have to improve the security status by using a security dashboard (Dogaheh, 2010). The reports and dashboards have to be on the need for information security managers (Wilkin and Chenhall, 2010) but there are no standards for the content of such dashboards (Bayuk and Mostashari, 2013). The *lack of structure* is related to the first problem and causes in the high diversity and complexity of the information security problem which causes uncertainty and confusion among top managers (Savola, 2007; 2009; von Solms et al., 1994; Willison and Backhouse, 2006). This causes in the fact, that managers do not make decisions based on data but on their experience, judgment and their best knowledge (Chai et al., 2011). Therefore, current research asks for a comprehensive approach to information security management (Abu-Musa, 2010; Nazareth and Choi, 2015; Savola, 2007; 2009; 2013; Soomro et al., 2016; Tu and Yuan, 2014) which captures the definition of "factors that have a significant impact on the information security" (Bayuk, 2013; Leon and Saxena, 2010; Ransbotham and Mitra, 2009; Soomro et al., 2016) and the established relationships between these fundamental objectives (Dhillon and Torkzadeh, 2006; Hu et al., 2012; Soomro et al., 2016). This research addresses the described needs with the development of the first theory of interrelated MSFs, which give a basis for decision-makers to understand the complexity of information security on an abstract level and also could be the basis of multiple future needs also described in literature like the goal based security metrics development (Bayuk, 2013; Boss et al., 2009; Diesch et al., 2018; Hayden, 2010; Jafari et al., 2010; Johnson and Goetz, 2007; Pendleton et al., 2017; Savola, 2007; Zalewski et al., 2014).

3. Methodology

To develop a comprehensive model of information security factors for decision makers the methodology of this work consists of two steps. Fig. 1 illustrates the steps. The first step is to find relevant literature with the help of a literature search process described in Section 3.1. The second step is to analyze the relevant literature for factors which have an influence on information security decisions. The results are categorized and high-level impact factors which are derived from literature. This step is illustrated in Section 3.2. The third step contains a semi-structured expert interview in order to evaluate the relevance of the impact factors in practice and explore interdependencies between them. The results are evaluated and relevant MSFs in practice as well as interdependencies which results in the comprehensive model of MSFs for decision-makers. In Section 3.3 the description of the expert interview methodology is shown.

3.1. Literature search

The search process is performed based on the method of Webster and Watson (2002). The literature search consists of the search scope followed by a keyword-search which ends in a forward and backward search. To provide high-quality articles, the scope is set to highly ranked journals within the information security domain and the information systems management domain because of the relation to the management view. Journals of the management domain were selected from the Senior Scholars' Basket of Journals (AIS Members, 2011). The journals of the security domain were selected from the Scimago Journal & Country Rank (SJR) (SJR, 2018) with the condition that they need to be part of the following categories: security, safety, risk or reliability. To not limit the search only to Journals, the scope was extended to several databases. These are ScienceDirect, OpacPlus and Google Scholar. OpacPlus is a wrapper of multiple databases including Scopus, Elsevier, Wiley, and ACM Digital Library. The results of Google Scholar were limited by 100 hits because the most relevant articles can be found within the first sites (Silic and Back, 2014). After the scope definition, the following search string was used to find articles: "(it OR information OR cyber)AND (resilience OR security)AND (factors OR kpi OR measures OR metrics OR measurement OR indicator OR management)". Because the management literature is not information security specific, the search string of these journals was adjusted to the first two parts: "(it OR information OR cyber)AND (resilience OR security)". Another adjustment

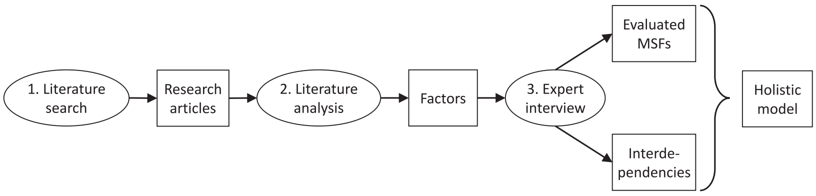

Fig. 1. Methodology of theory development.

was done by searching just for the title and abstract within information security specific sources because of the underlying diverse topic. The selection of relevant articles out of the first keyword search was done based on the title and abstract. Including criteria was, that there are factors described or mentioned which are influencing information security decisions. The forward and backward search was applied to all selected articles while the forward search was based on the “cited by” function of Google Scholar. The literature identification methodology results in 136 articles. The complete search matrix with the applied source, the keyword-search hits and the selected relevant article numbers is shown in Appendix A.

3.2. Literature analysis

The analysis was done based on the “open-axial-selective” approach of Corbin and Strauss, 1990 which is a grounded theory approach based on Glaser and Strauss (1967) and was recommended as a rigorous method for analyzing literature (Wolfswinkel et al., 2013). This approach has the advantage, that the whole context of an article can be analyzed in order to extract factors. Webster and Watson (2002) also support a literature analysis but with the categorization of a whole article in order to identify gaps in the literature, pointing out the state of the art and explaining past research. To extract specific knowledge and categorize this, the coding on a textual level of articles is more appropriate in this case. The coding follows the following steps:

(1) Assignment of text segments to a “first-order code”. For example, the text segment those organizations that have had a systems security function for some time should use these assessment methods to validate the results of other methods and to cross-check that they have not overlooked some important vulnerability” (Wood, 1987) was assigned the cluster “vulnerability assessment” as a factor which influences information security.
(2) Combines synonymous and their meanings to a “second-order code”.
(3) Categorize the “second order codes” to clusters based on overlapping meanings (infrastructure overview and asset knowledge), overlapping functions (management support and management standards) or theoretical constructs (confidentiality, integrity, and availability).

3.3. Expert interview

Previous research has been criticized in order of missing support of reliability and validity by empirical studies (Siponen and Willison, 2009; Tu and Yuan, 2014). The first goal of the expert interview was to evaluate the factors of the literature and thus generate MSFs which are relevant in practice. The second and main goal is the exploration of interdependencies between MSFs to develop the comprehensive model of MSFs.

There are various ways to design an expert interview. This study is designed as a semi-structured interview (Bortz and Döring, 1995) to combine the advantages of structured and open interviews. The interviewer is able to give room for explanations but also ensures, that all answers are given. With these considerations, the expert interview itself consists of three steps which are the operationalization of the described goals (chapter 3.3.1), the selection of experts (Section 3.3.2) and the analysis of the expert interviews (Section 3.3.3).

3.3.1. Operationalization

The interview guide gives the interviewer an orientation and an analysis is more comparable than without any structure. To develop the survey instrument, the rules of good expert interviews were considered (Bortz and Döring, 1995). The beginning of the interview was done with an open question on the most important factor, the interviewee considers for the information security in the organization (*Q0*). The following areas were discussed with the experts to support the given goals and control as well as confirm the validity of the factors:

- Evaluationof factors:
  A discussion about the meaning of each factor from a practical perspective was done in order to evaluate the content of the factors (*Q1.1*). The practical relevance was tested by asking about the importance of each factor for the information security of the organization (*Q1.2*).
- Exploration of interdependencies:
  To explore the interdependencies between the factors and get insights into them, a discussion about the practical usage and how the experts deal with each factor was done (*Q2.1*). To crosscheck the given statements, experts were asked for each factor, if the factor has a direct impact on the information security of the organization (*Q2.2*).
- Control questions:
  Questions about the absence of not mentioned important factors (*Q3.1*) and if the experts consider a factor which was discussed to be unimportant (*Q3.2*) are used to control the completeness of the given factors and further confirm the explored results.

3.3.2. Expert selection

An expert is a person with specific practical or experimental knowledge about a particular problem area or subject area and is able to structure this knowledge in a meaningful and action-guiding way for others (Bogner et al., 2014). The selection of interviewees was derived by this definition. Therefore, an expert should have several years of experience in the field of information security which points to specific practical knowledge in the field of information security. The expert should have a leading position within the organization which testifies the ability to the meaningful and action-guiding structuring of the information for others. Also, a leading position supports the underlying comprehensive view which is required for the goal of this research. The selection results in 19 participants. They were mainly chief information security officers (12) and information security officers (4). The others were one chief executive officer, one chief information officer, and a technical delivery manager. All experts had 5 years of experience at minimum, 16 years at average and 30 years at maximum. This shows, that the selected interviewees meet the requirements and are suitable for this approach. The participants worked in the following industries at this point in time: finance, automotive, diversified, aircraft, metal and electrical, services, hardware and software, and others. All but one organization had more than 2000 employees. This was the result of the requirements for experts which mean, that the organization has to had at minimum an information security team, which is typically not available in small businesses.

3.3.3. Interview analysis

The interviews were analyzed according to Mayring (2015). The basis for each question was a full transcript of the interview. The process contains of the following steps:

1. Paraphrasing
    - Painting of components that do not contribute or have little content.
    - Standardize language level.
    - Generate grammatical short forms.
2. Generalization
    - Generalize paraphrases on an abstract level.
    - Generalize predicates in an equal form.
    - Generate assumptions in case of doubt.
3. Reduction (can be done multiple times)
    - Delete phrases which have the same meaning.
    - Combine phrases of similar meaning.
    - Select phrases that are very content-bearing.
    - Generate assumptions in case of doubt.

To analyze quantitative aspects or interdependencies, Mayring (2015) also suggests two methods which are called "valence or intensity analysis" (V) and "contingency or interrelation analysis" (I) and used to analyze the interviews. Both methods contain mainly the same steps:

1. Formulate a question.
2. Determine the material sample.
3. Define the variables (V) / text modules for interrelation (I)
4. Define the scale (V) / rules for interrelation (I)
5. Coding
6. Analysis
7. Presentation and interpretation

4. Management success factors

The prerequisite for a comprehensive model of MSFs is evaluated MSFs, which have an influence on information security decisions. In Section 4.1, the results of the literature analysis are shown. These are factors which have an influence on information security decisions from the literature perspective. After that, the factors have to be evaluated and proved for their relevance in practice which results in evaluated MSFs. These results are shown in Section 4.2.

4.1. Factors derived from the literature

The analysis of 136 relevant articles from the search methodology resulted in 188 first-order codes. A code is a tuple of "factor in literature"-"author". So for each author, the different impact factors were coded. These codes appear in the following situations:

(1) They appear **directly** within the literature. An example is the following sentence of Atoum et al. (2014) "enrich the framework in other related dimensions such as *human resource, organization structures, global governance, regulation regimes, awareness programs* and thus provide a more detailed framework". This result directly in the corresponding list of first order codes. Most of these direct codes appear in enumerations within the introduction or future work sections of the analyzed literature and are not further explained.

(2) The first order codes are part of a **theory**. The first order codes are part of a hypothesis construct with a underlying theory and are tested with quantitative or qualitative studies. A example work is Kankanhalli et al. (2003) which describes the impact of the organizational size, the top management support and the industry type on the information systems security effectiveness. This example results in the corresponding first-order codes.

(3) **Indirectly** within the articles or because of their focus. These appearances are derived from the overall classification of the articles or some descriptions within the text which are not directly mention the first order code but the meaning was chosen to name it. The article with the title "design and validation of information security culture framework" (AlHogail, 2015) is named "security culture" as a first-order code. A other example for indirect mentions is those organizations that have had a systems security function for some time should use these assessment methods to validate the results of other methods and to cross-check that they have not overlooked some important vulnerability" (Wood, 1987) which is "vulnerability assessment" as a first-order code.

The aggregation of the 188 first-order codes results in 44 second-order codes. The following aggregation criteria were identified:

(1) Articles describe often, that the codes have the **same meaning**. An example is given by Jafari et al. (2010) which described "Safeguards: Protective measures prescribed to meet the security requirements [...], synonymous with countermeasures". This in conjunction with "improving the overall information security state by selecting the best security countermeasures (controls) to protect their information assets" (Yulianto et al., 2016) are safeguards, countermeasures, and controls a second-order code.

(2) Certain first-order codes are **part of** or included in other first-order codes which results in a second-order code. Examples in literature are "Value delivery (i.e. cost optimization and proving the value of information security)" (Yaokumah, 2014), "aside from the personnel measures which focus on human behavior" (Sowa and Gabriel, 2009) or "threats, which form part of such risk" (Willison and Backhouse, 2006). This indicates, that threats are part of risks.

(3) First-order codes are aggregated in order of their **underlying object**. An example is "organizational size", "industry type" and "organizational structure" which are all features of an organization and thus are aggregated to the second-order code "organizational factors".

The aggregation of the second-order codes to clusters and thus the overall factors, influencing security decisions, is based on common theories in literature. An example is the theory of the protection goals of information security which is supported by various authors: "with a goal to compromise Confidentiality, Integrity, and Availability (CIA)" or "it also coincides with the Confidentiality-Integrity-Availability (CIA) framework" (Goldstein et al., 2011) or "one view, which gained especially wide popularity, is called C-I-A triad" (Zalewski et al., 2014). This theory results in the consolidation of protection goals in the factor "CIA".

The result of the literature analysis is 12 factors influencing security decisions, namely: "Vulnerability", "Compliance & Policy", "Risk", "Physical security", "Continuity", "Infrastructure", "CIA", "Security management", "Awareness", "Resources", "Access control" and "Organizational factors". The detailed codes and the aggregation steps are available in Appendix B.

The literature analysis confirms the assertions made in Section 2.3 which say that various individual factors are mentioned, enumerated or examined. However, up to now, there has been no comprehensive view on them, a discussion of the practical relevance is missing and the interdependencies of the factors among each other are not described. The result of this chapter gives an abstract view of current factors in literature, influencing information security decisions.

4.2. Evaluation of Factors

The explored factors of the last Section 4.1 are the basis for the following evaluation and therefore to transform these factors to MSFs for information security decision-makers. In Section 4.2.1 the practical view of experts on the factors is compared to the literature view which is derived out of the literature analysis in Section 4.1. In addition, challenges of practitioners are supported for each factor. The result of the relevance validation is present in Section 4.2.2. Section 4.2.3 contains the result of the control questions and thus confirm the validity and relevance of the explored factors.

4.2.1. Content validation of MSFs

The relevance of the factors in practice and their validity makes them to MSFs. The general context analysis (Section 3.3) was used to determine the practical usage and meaning of the different factors out of the literature. To analyze them, the scope was set to the whole interview transcripts while the main answers are given by the guiding question *Q1.1* of the interview guide. Because of the methodology design of a semi-structured interview, the challenges and problems of each factor in practice is a side-result and also reported here. The following itemization shows each MSF with a description of the literature view, a consolidated practical view and the challenges practitioners face regarding each MSF. The literature view is a consolidation of definitions and opinions out of the literature analysis 3.3.3. The practical view and the descriptions of the challenges are a consolidation of the main opinion of all 19 experts.

- **Vulnerability**
  1. **Literature:** The definition of a vulnerability in literature is generally a "weakness of an asset or control that can be exploited by one or more threats" (ISO/IEC, 2018). This definition is very generic and can be technical as well as non-technical. NIST gives a more detailed definition as a "weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source" (NIST, 2018a). Common usage of the term in the analyzed literature is, that vulnerabilities are technical in nature. More specifically, "a vulnerability is a software defect or weakness in the security system which might be exploited by a malicious user causing loss or harm" (Joh and Malaiya, 2011).
  2. **Practice:** Vulnerabilities from the management perspective are always technical in nature. Specifically, known vulnerabilities within systems and software are meant by them. The common understanding of the experts was that vulnerability is a topic of patch management and a problem of not patched systems. All organizations do have patch management in place and try to minimize the vulnerabilities in the infrastructure. The assessment of them is done with vulnerability-scanners, penetration-tests, automatic scans, audits and the definition of toxic software which is detected on systems. Patching and the elimination of vulnerabilities are done based on the given assessment methods.
  3. **Challenges:** A problem is, that the vulnerabilities have to be known first. Not just the knowledge of the vulnerabilities is a problem but also the knowledge of the assets and the whole infrastructure of an organization is a challenge in practice. Just if an organization knows the whole assets and infrastructure, it is possible to determine, if there are known vulnerabilities or not.
- **Infrastructure**
  1. **Literature:** Infrastructure does have different aspects. Components are technical systems which itself try to protect the underlying assets or are there to identify attacks. Examples are firewalls, intrusion detection systems, information visibility, compromise detection, defense modeling, and other solutions. A second important concern is the prevention of attacks without any known vulnerabilities. This includes architectural decisions to segment the network, limit open access points or external connections, harden the systems, encrypt the communication or clean configuration issues. Since these are no specific vulnerabilities but considered as weaknesses, this topic is a stand-alone factor.
  2. **Practice:** Some of the experts see this factor as a vulnerability-topic but most of them associate more than that with the infrastructure factor. It is about knowing all systems and software as well as the connections between them and if they are secured or not. It is also about the "hardening" of all available systems, make threat models and secure the infrastructure in each network layer. To accomplish that, the experts use hardening-guidelines, secure deployment, installation routines, design reviews and configuration management databases.
  3. **Challenges:** Problems are the complexity of the activity, that it is difficult to check the wright implementation of the hardening guidelines and the above-mentioned problem of the difficulty to know all available systems and their connections.
- **Compliance & Policy**
  1. **Literature:** Security policies are an "aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information" (NIST, 2013). All activities concerning compliance and policies like policy deployment, policy effectiveness, legal compliance, and regulatory requirements are subsumed in this factor. The literature describes also multiple characteristics for good and bad policies and controls which have an influence on the information security of organizations.
  2. **Practice:** This factor means the implementation of requirements which are given from external and internal. These include laws, policies from the management and requirements from standards to get certificates. Practitioners use frameworks to implement them and audits as well as self-assessments to check them. This frameworks and policies help organizations which have not the common knowledge to consider all aspects of security.
  3. **Challenges:** 100% compliance does not mean 100% secure. This factor alone does not help in case of security but without, it is not possible to make audits or push measures through.
- **Security management**
  1. **Literature:** This factor subsumes all process activities within the information security management system and operational tasks like change management, incident management, process effectiveness measurement and the implementation of security standards. All aspects of the Plan-Do-Check-Act

approach of the ISO/IEC 27000 (ISO/IEC, 2018) are part of the security management factor. The other part are strategic topics like goal definition, top management support, governance, and strategic alignment as well as the documentation of these activities. Also, an important aspect in literature is the communication with employees and the top management. The ISO/IEC 27000 defines security management as a "systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security to achieve business objectives" (ISO/IEC, 2018). This definition shows that the monitoring part is also established within this factor. There are different methods and processes described to continuously improve the information security of an organization. This covers the implementation of metrics and the topic of compromise detection.

2. **Practice:** There are two management approaches in place. The risk-based and the control-based approach. There are various processes in place to support the two different approaches. Therefore the experts control their management processes with audits and using the Plan-Do-Check-Act framework from the ISO/IEC 27000 (ISO/IEC, 2018). The next important aspect for the interviewees was the business (top) management support and their understanding of the risks the organization is facing.
3. **Challenges:** A problem is the missing knowledge of concepts behind the security processes and also the lack of knowledge of available actions for improvements. The security management does not have an impact on the security of an organization without this knowledge.

- **Awareness**
  1. **Literature:** The definition of awareness in literature is to be aware of security concerns (NIST, 2013). Awareness in academic literature is discussed in different subjects. Including in this factor are behavioral topics like employee behavior, user activities, user interaction but also user reaction, user errors, and faults. All parts depending on knowledge like skills, education, training, and competence are also including in the awareness factor. Awareness in literature is not just about peoples behavior but also the personal needs of them, privacy issues, trust concerns as well as cultural thoughts and the social environment.
  2. **Practice:** All topics that concerning people and can not be treated with technology are subsumed by awareness. Typical understanding is the employee as a vulnerability with human errors, human behavior or not enough knowledge. A typical countermeasure is web-based and conventional training. Practitioners test their employees with own phishing-campaigns or check click-rates on their proxy-servers. Cultural and privacy concerns are not often taken into consideration.
  3. **Challenges:** Challenge in practice is, that awareness activities are very resource heavy and the effects are not that huge. Countermeasures often do not lead to measurable effects, they lead to annoyed employees and therefore, employees more often fail the same tests.
- **Risk**
  1. **Literature:** The risk factor is discussed as an overall risk management concern with possible threats, the likelihood of their occurrence and the possible impact on the organization. Literature mostly discusses the risk management process and the possible handling of present risks like prevention, tolerance, exposure, prediction, and perception. A comprehensive definition is given by the NIST SP800-37: "A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence" (NIST, 2018a).
  2. **Practice:** Experts use the same definition and understanding of risk as in literature. A risk is a severity and likelihood combined with an issue. Information security is the applied risk management because it is used to prioritize and define countermeasures. Therefore, all of the experts have risk management based on certain standards like ISO/IEC 27000 or NIST in place.
  3. **Challenges:** Not all risks can be mitigated, because of missing resources or other restrictions. Some managers also have problems to define risks which are understandable for technical employees or even for the top management. Also, the availability of the underlying data is a challenge in practice. An example of this is the consolidated view on possible threats. There are various technical solutions like threat intelligence platforms available on the market which helps to consolidate these data. The problem comes with the combination of the different factors to define the risk. A possible threat alone is not important for the information security management. The challenge is to analyze the underlying assets and their vulnerabilities and check if the threat can exploit one of these. After this combination, the risk can be defined and is useful for an information security manager.
- **Access control**
  1. **Literature:** Access control is not mentioned as a part of countermeasures. This topic is such important that it often emerges as an independent and important factor for security. Access control contains account management, software access control as well as access rights. It means "to ensure that access to assets is authorized and restricted based on business and security requirements" (ISO/IEC, 2018).
  2. **Practice:** Access control is the management and regulation of access to systems, applications, data, and infrastructure. It is not just about the access but also the key management, role administration, classification of data and the management of the identities within organizations. Therefore the experts have procedures per applications, try to implement the common principles like the need-to-know- or the least-privilege-principle. They check the available accesses, have identity and access management in place and use tools to monitor them.
  3. **Challenges:** Challenges occur in case of on-, off-boarding and department changes as well as the more and more open culture of organizations with "bring your own device" and "cloud infrastructure". Not just the open culture but also technologies and trends like the "internet of things" and "mobile devices" are increasingly a problem for this factor because each of these devices also has an identity. This increases the complexity of managing access control and has to be considered by choosing such technologies.
- **CIA**
  1. **Literature:** This factor is based on the overall theoretical construct of the protection goals of information security. Therefore the codings confidentiality, integrity, availability, as well as underlying goals like the non-repudiation, are subsumed in this factor. Articles about security metrics and security success are mostly based on this factor and plays a huge role in the security discussion.
  2. **Practice:** In practice, this factor is a theoretical construct with the same definition as in literature. It is used to communicate with the business management, to classify the need for protection or is not used in practice at all.
  3. **Challenges:** The problem in practice is that these classes can not be uniquely assigned to countermeasures. Many experts

consider this factor as an academic construct, which is outdated and not really practicable.

- **Organizational factors**
  1. **Literature:** The organizational factor itself means the properties of an organization which has an influence on the security of this organization. There are multiple authors which mentioned the influence of several factors like the organizational size, the industry type or the internal and external structure of the organization.
  2. **Practice:** These factor has the same meaning in practice like in literature. Most of the experts are not dealing with it because there are no possibilities to change the characteristic of the organization from their perspective. But it is considered in other factors like risks or in consideration of the implementation countermeasures. Practitioners say, that it might influence the possibilities of an organization.
  3. **Challenges:** A challenge is, that some attack surfaces are not influenced by any type of character an organization could have. A good example of this is ransomware which does not even look at the victim they attack.
- **Physical security**
  1. **Literature:** This factor have influence in reducing the opportunity to access assets physically in form of physical entry controls, the protection of the environment, building security with fences or other countermeasures, travel security and all activities around this. The literature does not mention this factor very often but consider it as really important for organizations and their management.
  2. **Practice:** Physical security is the physical protection of buildings, offices, servers, and hardware. It also contains the protection of the environment, persons, traveling and environmental disasters. Interviewees do work together with other departments dealing with this factor. It is mainly not the part of the security department of an organization.
  3. **Challenges:** The topic gets less important in times of the changing environment like mobile offices, roaming-users, home offices and cloud computing. This change brings with it other challenges.
- **Continuity**
  1. **Literature:** Continuity is split in business continuity and IT continuity. In case of cyber security, the term "refers to the ability to continuously deliver the intended outcome despite adverse cyber events" (Björck et al., 2015). The business continuity is on a more abstract level than cyber or it continuitiy and is defined as a "predetermined set of instructions or procedures that describe how an organization's mission-essential functions will be sustained [...] before returning to normal operations" (NIST, 2013). Resilience is not often represented in the literature and has already been identified as a research gap (Diesch et al., 2018).
  2. **Practice:** This factor is understood as the goal of the business as well as a partial goal of information security. Important is a continuous IT and a disaster and recovery plan which should be tested from time to time. There are opposite opinions in relation to business continuity management (BCM). Some experts say, that requirements come from the BCM to the information security management and others say, that they are being submitted to the BCM.
  3. **Challenges:** A challenge is finding a common understanding and effective communication between BCM and IT continuity.
- **Resources**
  1. **Literature:** Resources are not just money but also the availability of good skilled and well-educated employees. More general resources are "information and related resources, such as personnel, equipment, funds, and information technology" (NIST, 2013). The literature describes this factor as a limitation and mostly in a negative way. The perspective is given that, if you do not have enough resources, the organization is not able to implement security which as a negative influence. A second part is the cost-effectiveness of countermeasures and the return on security investments (ROSI).
  2. **Practice:** In practice, this factor is mostly addicted to budget, which has to be given by business management. A small part is also the number of employees with good knowledge and a appropriate education. Therefore, experts have applied budget-processes and recruitment campaigns. Cost-effectiveness and ROSI is not mentioned by the practitioners.
  3. **Challenges:** Problems are often in place of buying expensive tools and equipment in the security field and the argumentation of their adding value. It is often a tension between business management and security management.

Table 1
Importance of MSFs for the information security of organizations (number of experts).

MSF	not imp	rather not imp	rather imp	imp
Vulnerability	0	0	7	12
Resources	0	0	7	12
Awareness	1	0	6	12
Access Control	0	1	8	10
Physical Security	1	0	11	7
Infrastructure	0	1	12	6
Risk	0	1	12	6
Continuity	1	1	13	4
Security Management	3	1	8	7
Organizational	3	4	11	1
CIA Triad	7	1	8	3
Compliance & Policy	6	3	7	3

Partial aspects of individual factors are not covered by the literature or are not considered in practice. However, the contents and the understanding of the factors from the literature analysis agree with those of the experts. The challenges are not supported by all of the experts, because this was no explicit question. Thus, they were just included, if there are more than 2 mentions of the same challenge. The challenges further indicate, that a comprehensive model of them could help, improving the understanding of information security within organizations and also to help, improving specific factors.

4.2.2. Relevance validation of MSFs

The "valence or intensity analysis" (Section 3.3) was used to not just validate the factors concerning their content but also to determine their relevance in practice to the information security of an organization. Therefore, the scope of the analysis was also set to the whole interview transcripts but the main question supporting this validation is *Q1.2*. A 4-point Likert-scale which points out the importance of the factor for the information security of the organization is used. The coding of the scale is from not important (not imp) to important (imp). Table 1 shows an assorted view of the result. The assortion is based on the sum of the codings for "not important" and "rather not important" in conjunction with the sum of the coding "rather important" and "important", descending by the importance of the MSFs.

This result support, that all factors are relevant in practice. The last three factors are "Organizational factors", "CIA" and "Compliance & Policy". For all of them, the experts do have an explanation, why they are less important than the other factors. "Compliance & Policy" are not important for the information security of the organization itself but are necessary to comply with the law, to enforce countermeasures and to align the top management of the organization. The "CIA" factor is a goal factor and is useful to com-

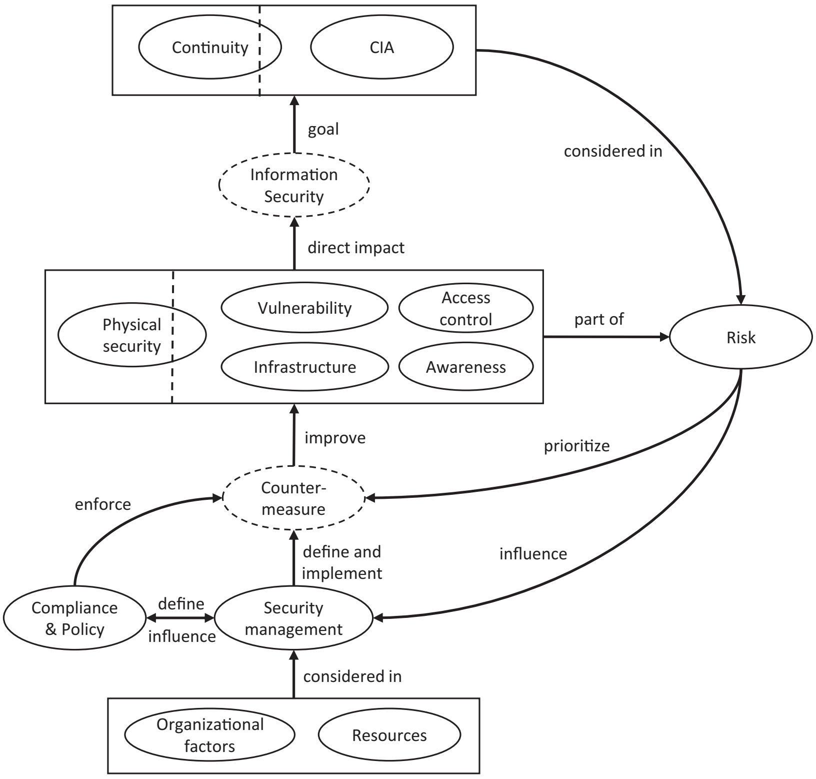

Fig. 2. A comprehensive model of MSFs for information security decision-makers.

municate and explain different risks or attacks and their impacts. “Organizational factors” are less important because there are cases, in which these factors are important but there are also attack scenarios in which this factor is not important. The management has to consider all the factors in order to make good decisions. The proposed factors are valid in their context as well as relevant in practice for decision-makers and thus are now called management success factors (MSFs).

4.2.3. Control questions

The main control questions *Q3.1* and *Q3.2* are used to ask for factors, which are important to make decisions and are not present in the interview guide as well as a consideration of the most unimportant factor. The most experts (12) do not have a factor, which is really unimportant. The only mentions of factors were the “Compliance & Policy” as well as “CIA” which agree with the ranking on the previous result. The question of missing factors results in a similar situation like before. 10 experts do not mention missing factors. The other factors which are missing are “management support”, “external interfaces”, “threat landscape” and “strategy” which are part of the coding and thus included in the aggregation of the literature analysis.

5. A comprehensive model of MSFs

The purpose of this research was the development of a comprehensive model of MSFs for information security decision makers. This result section combines the previous results with evaluated and relevant MSFs and adds interdependencies between them. The interdependencies were explored with the help of the “contingency or interrelation analysis” method (Section 3.3). The scope is the whole interview which was analyzed. The following text modules are examples to identify interrelations:

- ...have a direct impact on...
- ...is a basis to...
- ...is essential for...
- ...is the goal from...
- ...is considered in...

Fig. 2 shows all MSFs with their interrelations based on the expert interview. Solid ovals are representatives for the MSFs. Dotted ovals are representatives of concepts necessary to explain certain interdependencies. In this case, “Information security” is the representative for the information security status of an organization. The statement behind this is, that certain factors do have a direct impact on the information security status of the organization. The dotted oval “Countermeasures” is a part of the factor “Security management” but have important interdependencies which are explained by the experts. Thus, the security management itself does not have a huge impact on other factors, but they define and implement countermeasures which do have an influence on the MSFs given in the figure. Rectangles within the picture clusters multiple MSFs with the same interdependency to other MSFs. The dotted line within the rectangles indicates, that all MSFs which are left of this line, are not the primary part of the information security department of an organization. They are from other departments like the cooperate-security in the case of “Physical security” and the business continuity in case of “Continuity”. However, the collaboration between the departments is very close and the MSFs must certainly be considered in information security as well.

Key security indicators. The term key security indicator is not present in literature but is mentioned by practitioners. Key security indicators are MSFs, which have a direct impact on the security status of the organization. Therefore, the rectangle which includes the MSFs "Physical security", "Vulnerability", "Access control", "Awareness" and "Infrastructure" are key security indicators. Because of the direct connection to the information security concept, these factors are considered as indicators of the actual information security status of an organization. Security management has to implement countermeasures to actively improve these factors. These are the most important factors because of their direct impact.

Security goals. The MSFs "Continuity" and "CIA" are the protection goals of information security. This cluster is considered in the "Risk" MSF by data classification as well as a communication instrument which describes the impact of certain risks to top managers or technical employees. Disasters and continuity thoughts are also considered as risks which are the basis for recovery plans. The security goals are considered as the least important part of the MSF model by experts (Section 4.2.2) because they do not actively improve the security status and just help by prioritizing risks and communicate them to the business management.

Risk. The MSF "Risk" have the most interrelations and is the basic input for "security management". It uses security goals like described before. A prerequisite and a part of risks are key security indicators. They show the current information security status of which weaknesses were deriving. This, in combination with possible threats, the impact on the organization, and the likelihood of occurrence is a risk. Risks are influencing the "Security management" and is a basis to prioritize and define "Countermeasures". The management mostly uses standards and best practices like the ISO/IEC 27000 (ISO/IEC, 2018), NIST SP800-30 (NIST, 2015), NIST SP800-37 (NIST, 2018a) or others to deal with risks and derive countermeasures in a structured way.

Security management. The cluster with "Organizational factors" as well as "Resources" are MSFs which cannot be directly influenced by the experts. They are either given in case of "Organizational factors" or are set by the business management in case of "Resources". They are considered in the "Security management" in conjunction with the "Risk" MSF which are the basis to develop and implement countermeasures which should improve the key security indicators. "Compliance & Policy" are aids which help to enforce countermeasures with employees and are necessary to comply with laws. "Compliance & Policy" is split into external and internal rules which causes the interdependency in both ways to and from the "Security management" MSF. "Security management" define rules and external rules are influencing the "Security management". These rules are considered as the least important by the experts (Section 4.2.2) because they are not actively improving the security situation but are helpful to enforce countermeasures and help to deal with the topic.

6. Discussion and future research

The results of this research propose a comprehensive model of MSFs with their interdependencies for information security decision-makers. The MSFs were supposed based on the literature and are evaluated by experts from practice. These interviews also support interdependencies between the MSFs. The combination of these results in the development of the comprehensive model of MSFs.

Practitioners, as well as the literature, stated the need for a comprehensive view of the information security of organizations. The proposed model does support an abstract and comprehensive view of the complex topic of information security from the management perspective. The different MSFs are not explained in great detail but the interdependencies between them and the overall decision-making process are present in this research. The model gives a basis to decision-makers, which with information security management and help to decide if certain countermeasures are necessary or even useful. It is not just a basis for security managers but also for the business management as well as technical employees. With the help of this model, they are able to understand the difficulties and retrace certain decisions better. A better understanding also leads to better alignment and awareness.

The results are related to several other studies. Past literature does support a great explanation and study of different factors in detail and stated the importance of them. Studies also deal with models of different factors like awareness and their components. This research supports a comprehensive overview of high-level factors (MSFs) and a validation of them as well as a discussion of the relevance of these factors which has been criticized as missing in past articles. The research adds value to the research community by exploring interdependencies between the evaluated MSFs and propose a comprehensive model from the perspective of information security decision-makers. Best practices and standards are very generic and mostly describe processes. But, a complete implementation does not necessarily lead to better security and the standards have been criticized, also by experts in the interview, that they are just frameworks to be compliant. The interdependencies of the comprehensive model in this research help to decide which countermeasures are appropriate and which are not necessary. The standards and best practices give action proposals for improvements of the MSFs and thus complete this research with the next step after the decision was made.

Current standards and best practices, for example, the ISO/IEC 27000-series, the NIST SP800-series or the ISF are important to structure the processes of improving the information security of an organization. These documents either describe processes based on a risk management approach to implement countermeasures or define controls which have to be implemented to comply with the standard. The most experts in the interviews said that they combine two or more of them and uses the concepts they need or are appropriate for them to improve the information security status of the organization. The proposed model in this research contributes to these standards by improving the overall understanding and the interdependencies between the concepts described in the standards. Also, the model is a possibility to report the information security status based on the MSFs. Such a reporting is missing in the current standards and best practices as well as in research articles. The missing reporting standard or suggestions for that is a need which all of the interviewed experts have. Experts also struggle to report the information security decisions and status to the business management in an abstract and understandable way. The current solution of the interviewed experts is that they develop their own reporting standard. These reports do not contain aspects which can be compared with other businesses or even business units. The results of this research support these needs and can be used as a basis for such a reporting standard. Experts also looking for dedicated technical solutions like threat intelligence platforms, security incident management systems and information on indicators of compromise to mention just three. These technologies help to consolidate various information and present them to the management. Each technology is useful for a specific area. This research can help to argue the implementation of specific technologies, to illustrate their role in the overall security context and to identify gaps within the security landscape of an organization in which technologies could help.

The result can also be interpreted from the perspective of the information security status of an organization. From this perspective, the model indicates, that the key security indicators are important to improve the information security status of the organization. This interpretation in mind, small- and medium-sized businesses with fewer resources and not that much competence could implement light-weight countermeasures, which focus on the key security indicators. It could be a quick-win for the decisions in those organizations to focus on the key security indicators. This does not mean, that the standards and best practices or even the other factors of the model should be ignored by small- and medium-sized business. To continuously improve and monitor the information security status in a structured way, the processes and concepts of these standards have to be implemented and used. The proposed model can help these businesses and their management with less expertise in the field of security to understand the interdependencies between relevant concepts, understand which factors are influential and also which factors a manager has to consider by making decisions. Even which factors have to keep in mind to make well-informed decisions.

This study uses a mixed method approach with a literature analysis followed by a semi-structured interview to generate the results. Although a rigorous methodology was used, the study has several limitations. Despite the validation and the discussion with experts, a bias in the interpretation of the texts and the creation of the codes cannot be excluded. Surveyed experts are mainly active in large organizations. Some of them were previously employed in smaller businesses, but the inclusion of opinions from managers of smaller organizations could change the outcomes and importance of individual factors.

The results give many opportunities for future research. The proposed model is based on interdependencies, which are explored by a qualitative study. The interdependencies should be further tested with quantitative approaches to ensure their validity. Certain MSFs were clustered into rectangles. There could be interdependencies between the containing MSFs on deeper levels, which are not be explored in this study. Also, a look deeper within the certain proposed MSFs would be a possibility for future research. Open question from past literature could be solved with a more focused approach based on this results. Leon and Saxena (2010) identified a gap of the security metrics approach, which was not goal-focused in the past and suggested the development of a goal-list which could improve further security metrics development. This comprehensive model and their MSFs could be considered as a list of security goals from the management perspective and thus can be the basis of such research. Also, past metric approaches are mainly based on the individual security processes and thus is not appropriate for cross-organizational comparisons (Bayuk, 2013). A metrics approach based on a comprehensive model could be suitable for this. Also, the interview partner requested a dashboard and reporting standard for key security indicators which is not present in standards, best practices or research articles. To reduce the shortcomings, a future study is possible, which includes small- and medium-sized businesses and integrate them in the proposed model.

Information security managers should consider all the explored MSFs by taking decisions. The countermeasures and processes should not only be adopted because of their appearance in standards and best practices, but they should appropriate in the given situation. A common practice is also the fallback to risk acceptance (Bayuk, 2013) which do not improve the security status at all but is very easy to implement. The results of this study facilitate the understanding of the complex topic of information security and enable more people to make appropriate decisions and take the right actions within their current situation.

7. Conclusion

This research is suggesting a comprehensive model of management success factors (MSFs) for information security decision-makers. Therefore, a literature analysis with an open-axial-selective approach of 136 articles is used to identify factors which have an influence on the information security decisions of managers. A validation of these factors, as well as the check for their relevance, was supported by conducting an interview series of 19 experts from practice. This results in 12 MSFs. To finally develop the comprehensive model, the interviews are the basis to explore interdependencies between the MSFs.

This research suggests that “Physical security”, “Vulnerability”, “Access control”, “Infrastructure” and “Awareness” are key security indicators which have a direct impact on the information security status of an organization. The “Security management” have to consider “Risks”, “Organizational factors” and available “Resources” in order to generate countermeasures, which have an influence on the key security indicators. “Compliance & Policy” is an aid to enforce countermeasures and be compliant with laws. The well discussed MSF “Risk” is considering the security goals “CIA” and “Continuity” and also is using key security indicators to determine a risk level which is used to prioritize countermeasures.

This research offers a high-level view of the complex topic of information security decision-making from the perspective of security management experts. The comprehensive model of MSFs helps them and other employees as well as the business management to better understand the security needs and certain decisions in this context and thus improve their awareness. Future development of goal-oriented metrics and methods to quantify the status of information security as well as methods to aggregate them based on the key security indicators are not just interesting in research but also asked by practitioners.

Declaration of Competing Interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Appendix A

Table 2
Literature search matrix.

Resource	Hits	Relevant
MIS Quarterly	7	1
European Journal of Information Systems	20	3
Information Systems Journal	27	4
Information Systems Research	22	5
Journal of AIS	11	5
Journal of Information Technology	25	0
Journal of Management Information Systems	1	0
Journal of Strategic Information Systems	14	5
Journal of Management Information Systems	26	2
Decision Sciences	18	2
Information & Management	53	5
Information and Computer Security	99	10
IEEE Trans. on Dependable & Secure Computing	8	1
IEEE Trans. on Information Forensics and Security	7	0
Computers & Security	84	15
Google Scholar	100	11
ScienceDirect	41	6
OpacPlus	110	19
Backward		10
Forward		32
SUM	**673**	**136**

Appendix B

Table 3
Vulnerability.

First-order code	Second-order code	Cluster
technical vulnerabilities (Arora et al., 2010; Boss et al., 2009; Dzazali et al., 2009; Kraemer et al., 2009; NIST, 2008; Premaratne et al., 2008; Sowa and Gabriel, 2009; Straub and Welke, 1998; Sunyaev et al., 2009; Tashi and Ghernaouti-Hélie, 2008; Yeh and Chang, 2007)	technical vulnerabilities	Vulnerability
vulnerability assessment (Coronado et al., 2009; Gosavi and Bagade, 2015; Jafari et al., 2010; Siponen and Willison, 2009; Wood, 1987)		
network vulnerability (Gao and Zhong, 2015; Geer et al., 2003; Idika and Bhargava, 2012)		
system vulnerability (Boyer and McQueen, 2007; Dogaheh, 2010; Goldstein et al., 2011; Hayden, 2010; Holm and Afridi, 2015; Jean Camp and Wolfram, 2004; Lee and Larsen, 2009; Norman and Yasin, 2013; Pendleton et al., 2017; Pudar et al., 2009)		
vulnerability disclosure (Ransbotham and Mitra, 2009)		
host vulnerability (Idika and Bhargava, 2012)		
security problem (Straub and Welke, 1998)		
vulnerability(Alavi et al., 2016; Alqahtani, 2015; Ashenden, 2008; Azuwa et al., 2017; Bayuk and Mostashari, 2013; Bayuk, 2013; Ben-Aissa et al., 2012; Crossler and Belanger, 2012; Fenz et al., 2014; 2013; Hajdarevic and Allen, 2013; Hajdarevic et al., 2012; Herzog et al., 2007; Hua and Bapna, 2013; Ifinedo, 2012; Johnson and Goetz, 2007; Leon and Saxena, 2010; Mazur et al., 2015; Mermigas et al., 2013; Muthukrishnan and Palaniappan, 2016; Nazareth and Choi, 2015; Posey et al., 2015; Savola and Heinonen, 2011; Tanna et al., 2005; Vaughn et al., 2003; Verendel, 2009; von Solms and van Niekerk, 2013; Wang et al., 2013; Yeh and Chang, 2007; Young et al., 2016; Zalewski et al., 2014)		
it security (Björck et al., 2015; Manhart and Thalmann, 2015; Willison and Backhouse, 2006)	technical security	
technology (AlHogail, 2015; Ashenden, 2008; Goel and Chengalur-Smith, 2010; Goldstein et al., 2011; Gonzalez and Sawicka, 2002; Hall et al., 2011; Herrera, 2005; Jafari et al., 2010; Katos and Adams, 2005; Kraemer et al., 2009; Leon and Saxena, 2010; Merete Hagen et al., 2008; Nazareth and Choi, 2015; Norman and Yasin, 2013; Trèek, 2003; Yulianto et al., 2016)		
technical security (Azuwa et al., 2017; Coronado et al., 2009; Crossler et al., 2013; Dinev et al., 2009; Fenz et al., 2014; Gao and Zhong, 2015; Gosavi and Bagade, 2015; Hajdarevic et al., 2012; Hedström et al., 2011; Ifinedo, 2012; Manhart and Thalmann, 2015; Montesdioca and Maçada, 2015; Savola, 2007; Savola and Heinonen, 2011; Soomro et al., 2016; Sowa and Gabriel, 2009; Tu and Yuan, 2014; Uffen and Breitner, 2013; Vaughn et al., 2003; Veiga and Eloff, 2007; von Solms and von Solms, 2004; von Solms et al., 1994)		
application defect (Geer et al., 2003)	application security	
application security (Anderson and Moore, 2006; Bayuk, 2013; Dzazali et al., 2009; Fenz et al., 2014; Goel and Chengalur-Smith, 2010; Hajdarevic and Allen, 2013; Hajdarevic et al., 2012; Joh and Malaiya, 2011; Mazur et al., 2015; Mijnhardt et al., 2016; Muthukrishnan and Palaniappan, 2016; Yeh and Chang, 2007)		
feature security (Ransbotham and Mitra, 2009)		
patch coverage (Arora et al., 2010; Bayuk, 2013; Crossler and Belanger, 2012; Geer et al., 2003; Joh and Malaiya, 2011; Muthukrishnan and Palaniappan, 2016; Pendleton et al., 2017; Ransbotham and Mitra, 2009)		
software problem (Gupta and Hammond, 2005)		

Table 4
Physical security.

First-order code	Second-order code	Cluster
physical security (Collier et al., 2016; Dzazali et al., 2009; Ernest Chang and Ho, 2006; Fenz et al., 2014; Goldstein et al., 2011; Gosavi and Bagade, 2015; Hajdarevic and Allen, 2013; Hajdarevic et al., 2012; Hong et al., 2003; Kankanhalli et al., 2003; Mazur et al., 2015; Mijnhardt et al., 2016; Narain Singh et al., 2014; Norman and Yasin, 2013; Pudar et al., 2009; Sowa and Gabriel, 2009; Trèek, 2003; Tu and Yuan, 2014; von Solms et al., 1994; Wang and Wulf, 1997; Willison and Backhouse, 2006)	physical security	Physical security
physical access (LeMay et al., 2011; Trèek, 2003)		
physical environment (Jafari et al., 2010; Smith et al., 2010; Veiga and Eloff, 2007; Yeh and Chang, 2007)		

Table 5
Compliance & Policy.

First-order code	Second-order code	Cluster
organizational compliance (Jean Camp and Wolfram, 2004)	policy	Compliance & Policy
policy compliance (Crossler et al., 2013; Hall et al., 2011; Hong et al., 2003; Hu et al., 2012; Ifinedo, 2012; Johnston et al., 2016; Smith et al., 2010; Trèek, 2003)		
policy (Abu-Musa, 2010; Alavi et al., 2016; Ashenden, 2008; Bayuk and Mostashari, 2013; Boss et al., 2009; Cavusoglu et al., 2004; Dzazali et al., 2009; Ernest Chang and Ho, 2006; Goel and Chengalur-Smith, 2010; Hayden, 2010; Hedström et al., 2011; Herath and Rao, 2009; Herrera, 2005; Hong et al., 2003; Horne et al., 2017; Idika and Bhargava, 2012; Jafari et al., 2010; Johnson and Goetz, 2007; Katos and Adams, 2005; Knapp et al., 2009; Kotenko and Bogdanov, 2009; Kotulic and Clark, 2004; Kraemer et al., 2009; Lowry and Moody, 2015a; 2015b; Merete Hagen et al., 2008; Mijnhardt et al., 2016; Mishra and Chasalow, 2011; Montesdioca and Maçada, 2015; Narain Singh et al., 2014; Nazareth and Choi, 2015; Norman and Yasin, 2013; Ransbotham and Mitra, 2009; Sharman et al., 2004; Soomro et al., 2016; Straub and Welke, 1998; Tashi and Ghernaouti-Hélie, 2008; Tsiakis and Stephanides, 2005; Tu and Yuan, 2014; Uffen and Breitner, 2013; Vaughn et al., 2003; Veiga and Eloff, 2007; von Solms and von Solms, 2004; von Solms et al., 1994; Wang et al., 2013; Willison and Backhouse, 2006; Wood, 1987; Yeh and Chang, 2007)		
security compliance (Crossler et al., 2013; Dzazali et al., 2009; Ernest Chang and Ho, 2006; Fenz et al., 2014; 2013; Hayden, 2010; Herath and Rao, 2009; Ifinedo, 2012; Karjalainen and Siponen, 2011; Kraemer et al., 2009; Lowry and Moody, 2015a; Mijnhardt et al., 2016; Narain Singh et al., 2014; Sharman et al., 2004; Soomro et al., 2016; Tu and Yuan, 2014; Willison and Backhouse, 2006; Yulianto et al., 2016)		
legal requirements (Alavi et al., 2016; Dzazali et al., 2009; Knapp et al., 2009; Kraemer et al., 2009; Manhart and Thalmann, 2015; Savola and Heinonen, 2011; Sunyaev et al., 2009; Uffen and Breitner, 2013; von Solms and von Solms, 2004)	compliance	
law compliance (Hall et al., 2011; Hong et al., 2003; Johnson and Goetz, 2007; Leon and Saxena, 2010; Merete Hagen et al., 2008; Tariq, 2012; Veiga and Eloff, 2007; Yeh and Chang, 2007)		
legislation (Tashi and Ghernaouti-Hélie, 2008; Trèek, 2003)		
regulatory requirements (Abu-Musa, 2010; Atoum et al., 2014; Bayuk and Mostashari, 2013; Fenz et al., 2013; Norman and Yasin, 2013)		
regulatory compliance (Horne et al., 2017; Narain Singh et al., 2014)		

Table 6
Risk.

First-order code	Second-order code	Cluster
risk management (Ashenden, 2008; Bayuk and Mostashari, 2013; Bayuk, 2013; Beresnevichiene et al., 2010; Collier et al., 2016; Coronado et al., 2009; Ernest Chang and Ho, 2006; Fenz et al., 2014; 2013; Gao and Zhong, 2015; Geer et al., 2003; Hajdarevic and Allen, 2013; Hajdarevic et al., 2012; Hall et al., 2011; Horne et al., 2017; Kotulic and Clark, 2004; Leon and Saxena, 2010; Lowry and Moody, 2015a; Manhart and Thalmann, 2015; Mazur et al., 2015; Merete Hagen et al., 2008; Mijnhardt et al., 2016; Nazareth and Choi, 2015; NIST, 2008; Norman and Yasin, 2013; Ransbotham and Mitra, 2009; Savola, 2007; 2009; Savola and Heinonen, 2011; Sowa and Gabriel, 2009; Straub and Welke, 1998; Tu and Yuan, 2014; von Solms et al., 1994; Wang et al., 2013; Wilkin and Chenhall, 2010; Yaokumah, 2014; Yeh and Chang, 2007)	risk management	Risk
risk prevention (Hall et al., 2011; Veiga and Eloff, 2007)		
risk tolerance (Liang and Xue, 2009)		
risk exposure (Mermigas et al., 2013)		
risk prediction (Fenz et al., 2014)		
software risk (Boss et al., 2009; Tanna et al., 2005)		
system risk (Chai et al., 2011; Pendleton et al., 2017; Willison and Backhouse, 2006)		
risk perception (Vance et al., 2014)		
risk assessment (Abu-Musa, 2010; Alavi et al., 2016; Azuwa et al., 2017; Cavusoglu et al., 2004; Chai et al., 2011; Dogaheh, 2010; Fenz et al., 2014; Goldstein et al., 2011; Gonzalez and Sawicka, 2002; Gosavi and Bagade, 2015; Hayden, 2010; Hong et al., 2003; Jean Camp and Wolfram, 2004; Joh and Malaiya, 2011; Johnson and Goetz, 2007; Knapp et al., 2009; Siponen and Willison, 2009; Straub and Welke, 1998; Sunyaev et al., 2009; Tashi and Ghernaouti-Hélie, 2008; Veiga and Eloff, 2007; Verendel, 2009; von Solms et al., 1994)		
risk analysis (Goel and Chengalur-Smith, 2010; Hua and Bapna, 2013; Kumar et al., 2008; Pudar et al., 2009; Sunyaev et al., 2009; Tsiakis and Stephanides, 2005; Young et al., 2016; Zobel and Khansa, 2012)		
local threats (Willison and Backhouse, 2006)	threats	
threat impact (Alqahtani, 2015; Holm and Afridi, 2015)		
available exploits (Holm and Afridi, 2015; Premaratne et al., 2008)		
possible threats (Abu-Musa, 2010; Alqahtani, 2015; Azuwa et al., 2017; Bayuk and Mostashari, 2013; Bayuk, 2013; Ben-Aissa et al., 2012; Boss et al., 2009; Collier et al., 2016; Coronado et al., 2009; Crossler and Belanger, 2012; Crossler et al., 2013; Dogaheh, 2010; Fenz et al., 2014; 2013; Gao and Zhong, 2015; Gosavi and Bagade, 2015; Gupta and Hammond, 2005; Hajdarevic and Allen, 2013; Hajdarevic et al., 2012; Hall et al., 2011; Herath et al., 2014; Herzog et al., 2007; Hu et al., 2012; Hua and Bapna, 2013; Ifinedo, 2012; Jafari et al., 2010; Johnston et al., 2016; Jones and Horowitz, 2012; Knapp et al., 2009; Lee and Larsen, 2009; Mazur et al., 2015; Muthukrishnan and Palaniappan, 2016; Nazareth and Choi, 2015; Norman and Yasin, 2013; Pendleton et al., 2017; Posey et al., 2015; Purboyo et al., 2011; Sowa and Gabriel, 2009; Sunyaev et al., 2009; Tariq, 2012; Tran et al., 2016; Trèek, 2003; Tsiakis and Stephanides, 2005; Tu and Yuan, 2014; Uffen and Breitner, 2013; Verendel, 2009; von Solms and van Niekerk, 2013; Young et al., 2016; Zobel and Khansa, 2012)		

Table 7
Continuity.

First-order code	Second-order code	Cluster
business continuity (Dzazali et al., 2009; Hong et al., 2003; Horne et al., 2017; Narain Singh et al., 2014; Smith et al., 2010; Sowa and Gabriel, 2009; Tashi and Ghernaouti-Hélie, 2008; Trèek, 2003; Veiga and Eloff, 2007)	business continuity	Continuity
business continuity plan (Ernest Chang and Ho, 2006; Mijnhardt et al., 2016; Tariq, 2012)		
resilience (Björck et al., 2015; Collier et al., 2016; Fenz et al., 2013; Johnson and Goetz, 2007; Tran et al., 2016; Zalewski et al., 2014; Zobel and Khansa, 2012)	it continuity	
survivability (Katos and Adams, 2005; Vaughn et al., 2003)		
contingency plan (Abu-Musa, 2010; von Solms et al., 1994; Wood, 1987)		
power failure (Gupta and Hammond, 2005)		
acts of god (Björck et al., 2015; Willison and Backhouse, 2006)		
natural disaster (Gupta and Hammond, 2005)		
restorability (Bayuk and Mostashari, 2013; Boyer and McQueen, 2007)	recovery	
disaster recovery (Crossler and Belanger, 2012; Hall et al., 2011; Kumar et al., 2008; Savola, 2009; Tariq, 2012; von Solms et al., 1994; Wilkin and Chenhall, 2010)		

Table 8
Infrastructure.

First-order code	Second-order code	Cluster
infrastructure administration (Hua and Bapna, 2013; Savola and Heinonen, 2011; Wood, 1987)	infrastructure overview	Infrastructure
secure environment (Abu-Musa, 2010; AlHogail, 2015; Ernest Chang and Ho, 2006; Gonzalez and Sawicka, 2002; Herath and Rao, 2009; Herrera, 2005; Liang and Xue, 2009; Mijnhardt et al., 2016; Narain Singh et al., 2014; Norman and Yasin, 2013; Posey et al., 2015; Trèek, 2003; von Solms et al., 1994; Wood, 1987)		
infrastructure security (Crossler and Belanger, 2012; Hong et al., 2003; Katos and Adams, 2005; Trèek, 2003)		
ict infrastructure (Cavusoglu et al., 2004; Fenz et al., 2013; Horne et al., 2017; Soomro et al., 2016)		
equipment (Sharman et al., 2004)		
hardware security (Yeh and Chang, 2007)		
network security (Azuwa et al., 2017; Bayuk and Mostashari, 2013; Bayuk, 2013; Gosavi and Bagade, 2015; Kotenko and Bogdanov, 2009; Mazur et al., 2015)	network security	
secure network communication (Azuwa et al., 2017; Fenz et al., 2014; Herzog et al., 2007; Premaratne et al., 2008; Ransbotham and Mitra, 2009; Smith et al., 2010; Yeh and Chang, 2007)		
cryptography (Geer et al., 2003; Herzog et al., 2007; Trèek, 2003; Wang and Wulf, 1997)		
encryption (Chai et al., 2011; Gosavi and Bagade, 2015; Gupta and Hammond, 2005; Ifinedo, 2012)		
network hardening (Idika and Bhargava, 2012)		
secure protocol (Ransbotham and Mitra, 2009)		
asset identification (Bayuk and Mostashari, 2013; Ernest Chang and Ho, 2006; Fenz et al., 2014; Jafari et al., 2010; Merete Hagen et al., 2008; NIST, 2008; Sharman et al., 2004; Trèek, 2003; von Solms and van Niekerk, 2013)	asset knowledge	
asset assessment (Boyer and McQueen, 2007; Gao and Zhong, 2015; Hajdarevic et al., 2012; Herzog et al., 2007; Jafari et al., 2010; Kraemer et al., 2009; Montesdioca and Maçada, 2015; Purboyo et al., 2011; Smith et al., 2010)		
asset management (Crossler et al., 2013; Hall et al., 2011; Hong et al., 2003; Horne et al., 2017; Ifinedo, 2012; Mijnhardt et al., 2016; Smith et al., 2010; Soomro et al., 2016; Veiga and Eloff, 2007)		
asset classification (Narain Singh et al., 2014)		
system configuration (Alavi et al., 2016; Bayuk, 2013; Geer et al., 2003; Hua and Bapna, 2013; Jafari et al., 2010; Jones and Horowitz, 2012; Kotenko and Bogdanov, 2009; Kraemer et al., 2009; Leon and Saxena, 2010; Muthukrishnan and Palaniappan, 2016)	system hardening	
system maintenance (Alavi et al., 2016; Ernest Chang and Ho, 2006; Hong et al., 2003; Ifinedo, 2012; Narain Singh et al., 2014; Nazareth and Choi, 2015; NIST, 2008; Smith et al., 2010; Sowa and Gabriel, 2009; Trèek, 2003; Veiga and Eloff, 2007; Wood, 1987)		
system weakness (Goldstein et al., 2011; LeMay et al., 2011; Purboyo et al., 2011; Vaughn et al., 2003)		
technology architecture (Björck et al., 2015; Cavusoglu et al., 2004; Johnson and Goetz, 2007; Knapp et al., 2009; Mijnhardt et al., 2016)	architectural factors	
firewall architecture (Sharman et al., 2004)		
system architecture (Jones and Horowitz, 2012; Soomro et al., 2016; Yeh and Chang, 2007)		
connections with public network (Johnson and Goetz, 2007; Sharman et al., 2004)	external connections	
access points (NIST, 2008)		
external system connections (Pudar et al., 2009; von Solms and van Niekerk, 2013)		

Table 9
Access control.

First-order code	Second-order code	Cluster
identity (Gosavi and Bagade, 2015; Mijnhardt et al., 2016; Savola and Heinonen, 2011; Wang and Wulf, 1997) **account management** (Anderson and Moore, 2006; Osvaldo De Sordi et al., 2014) **access control** (Abu-Musa, 2010; Azuwa et al., 2017; Bayuk and Mostashari, 2013; Beresnevichiene et al., 2010; Boyer and McQueen, 2007; Chai et al., 2011; Crossler and Belanger, 2012; Dhillon and Torkzadeh, 2006; Dogaheh, 2010; Dzazali et al., 2009; Ernest Chang and Ho, 2006; Geer et al., 2003; Herzog et al., 2007; Holm and Afridi, 2015; Hong et al., 2003; Ifinedo, 2012; Jafari et al., 2010; Mijnhardt et al., 2016; Narain Singh et al., 2014; Ransbotham and Mitra, 2009; Trèek, 2003; Veiga and Eloff, 2007; Willison and Backhouse, 2006) **access rights** (Sharman et al., 2004) **software access control** (LeMay et al., 2011; Smith et al., 2010; Wang and Wulf, 1997)	identity management access control	Access control

Table 10
Awareness.

First-order code	Second-order code	Cluster
personnel security (Ernest Chang and Ho, 2006; Goel and Chengalur-Smith, 2010; Herath and Rao, 2009; Herrera, 2005; Kankanhalli et al., 2003; Narain Singh et al., 2014; Ransbotham and Mitra, 2009; Smith et al., 2010; Sowa and Gabriel, 2009; Trèek, 2003; Uffen and Breitner, 2013; Vaughn et al., 2003; von Solms and von Solms, 2004; von Solms et al., 1994; Yeh and Chang, 2007) **awareness** (Abu-Musa, 2010; Alavi et al., 2016; Alqahtani, 2015; Ashenden, 2008; Atoum et al., 2014; Coronado et al., 2009; Dhillon and Torkzadeh, 2006; Dinev et al., 2009; Dzazali et al., 2009; Gao and Zhong, 2015; Hall et al., 2011; Hong et al., 2003; Jafari et al., 2010; Johnson and Goetz, 2007; Kankanhalli et al., 2003; Karjalainen and Siponen, 2011; Knapp et al., 2009; Kraemer et al., 2009; Manhart and Thalmann, 2015; Merete Hagen et al., 2008; Narain Singh et al., 2014; Norman and Yasin, 2013; Pendleton et al., 2017; Sharman et al., 2004; Soomro et al., 2016; Sowa and Gabriel, 2009; Straub and Welke, 1998; Tran et al., 2016; Tu and Yuan, 2014; Veiga and Eloff, 2007; Velki et al., 2014; von Solms and von Solms, 2004; Wang et al., 2013; Wilkin and Chenhall, 2010; Willison and Backhouse, 2006; Yeh and Chang, 2007; Zobel and Khansa, 2012) **people** (AlHogail, 2015; Gonzalez and Sawicka, 2002; Hall et al., 2011; Horne et al., 2017; Sharman et al., 2004; Yulianto et al., 2016) **technology awareness** (Dinev and Hu, 2007; Herath et al., 2014)	awareness	Awareness
training (AlHogail, 2015; Ashenden, 2008; Dogaheh, 2010; Karjalainen and Siponen, 2011; Lowry and Moody, 2015a; Merete Hagen et al., 2008; NIST, 2008; Posey et al., 2015; Sharman et al., 2004; Tran et al., 2016) **skills** (Alavi et al., 2016) **user knowledge** (Abu-Musa, 2010; Alqahtani, 2015; Fenz et al., 2014; Hajdarevic et al., 2012; Horne et al., 2017; Johnson and Goetz, 2007; Lowry and Moody, 2015b; Manhart and Thalmann, 2015; Nazareth and Choi, 2015; Posey et al., 2015; Veiga and Eloff, 2007; Wood, 1987) **education** (Kraemer et al., 2009; Willison and Backhouse, 2006) **it competence** (Ernest Chang and Ho, 2006; Tu and Yuan, 2014)	user knowledge	
user activities (Björck et al., 2015; Geer et al., 2003; Vance et al., 2014) **human interaction** (Kotenko and Bogdanov, 2009; Trèek, 2003) **human error** (Alavi et al., 2016; Kraemer et al., 2009; Vaughn et al., 2003) **user error** (Gupta and Hammond, 2005) **user/human behavior** (Boss et al., 2009; Crossler et al., 2013; Dinev et al., 2009; Dinev and Hu, 2007; Dogaheh, 2010; Gonzalez and Sawicka, 2002; Hedström et al., 2011; Herath and Rao, 2009; Hua and Bapna, 2013; Ifinedo, 2012; Johnston et al., 2016; Karjalainen and Siponen, 2011; Kraemer et al., 2009; Liang and Xue, 2009; Lowry and Moody, 2015a; Merete Hagen et al., 2008; Montesdioca and Maçada, 2015; Narain Singh et al., 2014; Soomro et al., 2016; Sowa and Gabriel, 2009; Uffen and Breitner, 2013; Vance et al., 2014; Veiga and Eloff, 2007; Velki et al., 2014; von Solms and van Niekerk, 2013) **criminal behavior** (Kankanhalli et al., 2003) **attack behavior** (Gao and Zhong, 2015; Pudar et al., 2009)	behavior	
ethical dimension (von Solms and von Solms, 2004) **work ethic** (Dhillon and Torkzadeh, 2006) **ethical environment** (Dhillon and Torkzadeh, 2006; Veiga and Eloff, 2007) **work situation** (Dhillon and Torkzadeh, 2006)	ethical factors	
security culture (Alavi et al., 2016; AlHogail, 2015; Ashenden, 2008; Boss et al., 2009; Collier et al., 2016; Dinev et al., 2009; Herath and Rao, 2009; Hu et al., 2012; Johnson and Goetz, 2007; Knapp et al., 2009; Kraemer et al., 2009; Merete Hagen et al., 2008; Narain Singh et al., 2014; Norman and Yasin, 2013; Tu and Yuan, 2014; Veiga and Eloff, 2007) **philosophical culture** (Yulianto et al., 2016)	culture	
personal privacy (Ben-Aissa et al., 2012; Boss et al., 2009; Coronado et al., 2009; Dhillon and Torkzadeh, 2006; Dogaheh, 2010; Fenz et al., 2013; Savola, 2009; Tariq, 2012; Wilkin and Chenhall, 2010) **trust** (Boss et al., 2009; Coronado et al., 2009; Dhillon and Torkzadeh, 2006; Dogaheh, 2010; Dzazali et al., 2009; Gao and Zhong, 2015; Horne et al., 2017; Johnston et al., 2016; Lowry and Moody, 2015b; Sowa and Gabriel, 2009; Tariq, 2012; Veiga and Eloff, 2007) **personal needs** (Dhillon and Torkzadeh, 2006) **individual belief** (Hu et al., 2012) **individual impact** (Norman and Yasin, 2013)	personal security	
usefulness / easy to use (Dinev et al., 2009; Dinev and Hu, 2007; Osvaldo De Sordi et al., 2014) **usability** (Bayuk, 2013; Dinev and Hu, 2007; Lee and Larsen, 2009; Verendel, 2009)	usability	

Table 11
CIA.

First-order code	Second-order code	Cluster
reliability (Ben-Aissa et al., 2012; Savola and Heinonen, 2011; Verendel, 2009; Wang and Wulf, 1997; Zalewski et al., 2014)	protection goals	CIA
authenticity (Azuwa et al., 2017; Ben-Aissa et al., 2012; Gosavi and Bagade, 2015; Holm and Afridi, 2015; Jafari et al., 2010; Katos and Adams, 2005; Savola, 2009; Savola and Heinonen, 2011; Trèek, 2003; Tsiakis and Stephanides, 2005; Wang and Wulf, 1997)		
accountability (Dhillon and Torkzadeh, 2006; Leon and Saxena, 2010; Wood, 1987)		
non-repudiation (Ben-Aissa et al., 2012; Jafari et al., 2010; Purboyo et al., 2011; Savola, 2009; Trèek, 2003; Tsiakis and Stephanides, 2005; Wang and Wulf, 1997)		
data integrity (Boyer and McQueen, 2007; Dhillon and Torkzadeh, 2006; Gupta and Hammond, 2005; Tariq, 2012)	integrity	
transaction integrity (Gupta and Hammond, 2005)		
process/organizational integrity (Dhillon and Torkzadeh, 2006)		
integrity (Abu-Musa, 2010; Ashenden, 2008; Bayuk and Mostashari, 2013; Ben-Aissa et al., 2012; Beresnevichiene et al., 2010; Cavusoglu et al., 2004; Dzazali et al., 2009; Ernest Chang and Ho, 2006; Goel and Chengalur-Smith, 2010; Goldstein et al., 2011; Hajdarevic and Allen, 2013; Hall et al., 2011; Hedström et al., 2011; Herath et al., 2014; Holm and Afridi, 2015; Hong et al., 2003; Horne et al., 2017; Hu et al., 2012; Hua and Bapna, 2013; Jafari et al., 2010; Joh and Malaiya, 2011; Knapp et al., 2009; Leon and Saxena, 2010; Mijnhardt et al., 2016; Mishra and Chasalow, 2011; Muthukrishnan and Palaniappan, 2016; Nazareth and Choi, 2015; Posey et al., 2015; Pudar et al., 2009; Purboyo et al., 2011; Savola, 2009; Savola and Heinonen, 2011; Sowa and Gabriel, 2009; Tariq, 2012; Tashi and Ghernaouti-Hélie, 2008; Trèek, 2003; Tsiakis and Stephanides, 2005; Tu and Yuan, 2014; Uffen and Breitner, 2013; von Solms and van Niekerk, 2013; Wang and Wulf, 1997; Wilkin and Chenhall, 2010; Yaokumah, 2014; Zalewski et al., 2014)		
available information (Dhillon and Torkzadeh, 2006)	availability	
availability (Abu-Musa, 2010; Ashenden, 2008; Bayuk and Mostashari, 2013; Ben-Aissa et al., 2012; Beresnevichiene et al., 2010; Cavusoglu et al., 2004; Dogaheh, 2010; Dzazali et al., 2009; Ernest Chang and Ho, 2006; Goel and Chengalur-Smith, 2010; Goldstein et al., 2011; Gupta and Hammond, 2005; Hajdarevic and Allen, 2013; Hall et al., 2011; Hedström et al., 2011; Herath et al., 2014; Holm and Afridi, 2015; Horne et al., 2017; Hu et al., 2012; Jafari et al., 2010; Joh and Malaiya, 2011; Knapp et al., 2009; Kraemer et al., 2009; Leon and Saxena, 2010; Mijnhardt et al., 2016; Mishra and Chasalow, 2011; Muthukrishnan and Palaniappan, 2016; Nazareth and Choi, 2015; Norman and Yasin, 2013; Posey et al., 2015; Pudar et al., 2009; Purboyo et al., 2011; Savola, 2009; Sowa and Gabriel, 2009; Tashi and Ghernaouti-Hélie, 2008; Tu and Yuan, 2014; Uffen and Breitner, 2013; von Solms and van Niekerk, 2013; Wang and Wulf, 1997; Zalewski et al., 2014)		
confidentiality (Abu-Musa, 2010; Ashenden, 2008; Bayuk and Mostashari, 2013; Ben-Aissa et al., 2012; Beresnevichiene et al., 2010; Cavusoglu et al., 2004; Dogaheh, 2010; Dzazali et al., 2009; Ernest Chang and Ho, 2006; Goel and Chengalur-Smith, 2010; Goldstein et al., 2011; Hajdarevic and Allen, 2013; Hall et al., 2011; Hedström et al., 2011; Herath et al., 2014; Holm and Afridi, 2015; Hong et al., 2003; Horne et al., 2017; Hu et al., 2012; Jafari et al., 2010; Joh and Malaiya, 2011; Knapp et al., 2009; Leon and Saxena, 2010; Mijnhardt et al., 2016; Mishra and Chasalow, 2011; Muthukrishnan and Palaniappan, 2016; Nazareth and Choi, 2015; Osvaldo De Sordi et al., 2014; Posey et al., 2015; Pudar et al., 2009; Purboyo et al., 2011; Savola, 2009; Sowa and Gabriel, 2009; Tashi and Ghernaouti-Hélie, 2008; Trèek, 2003; Tsiakis and Stephanides, 2005; Tu and Yuan, 2014; Uffen and Breitner, 2013; von Solms and van Niekerk, 2013; Wang and Wulf, 1997; Yaokumah, 2014; Zalewski et al., 2014)	confidentiality	

Table 12
Organizational factors.

First-order code	Second-order code	Cluster
organization size (Coronado et al., 2009; Ernest Chang and Ho, 2006; Kankanhalli et al., 2003; Kotulic and Clark, 2004; Lee and Larsen, 2009; Lowry and Moody, 2015b; Narain Singh et al., 2014; Norman and Yasin, 2013)	organizational factors	Organizational factors
organizational factors (AlHogail, 2015; Fenz et al., 2014; Herath and Rao, 2009; Hong et al., 2003; Kraemer et al., 2009; Leon and Saxena, 2010; Manhart and Thalmann, 2015; Savola, 2007; Soomro et al., 2016; Sowa and Gabriel, 2009; Sunyaev et al., 2009; Trèek, 2003; Tu and Yuan, 2014; Vaughn et al., 2003; Veiga and Eloff, 2007; von Solms and von Solms, 2004)		
organization structure (Abu-Musa, 2010; Atoum et al., 2014; Kotulic and Clark, 2004; Tu and Yuan, 2014; Yeh and Chang, 2007)		
industry type (Coronado et al., 2009; Dzazali et al., 2009; Ernest Chang and Ho, 2006; Kankanhalli et al., 2003; Narain Singh et al., 2014; Norman and Yasin, 2013; Yeh and Chang, 2007)		
external conditions (Sharman et al., 2004)	external factor	
reputation (Gao and Zhong, 2015; Osvaldo De Sordi et al., 2014; Tu and Yuan, 2014)		

Table 13
Security management.

First-order code	Second-order code	Cluster
countermeasures (measures) (Alavi et al., 2016; Crossler et al., 2013; Fenz et al., 2014; 2013; Herzog et al., 2007; Kotulic and Clark, 2004; Kumar et al., 2008; Leon and Saxena, 2010; Mermigas et al., 2013; Pendleton et al., 2017; Pudar et al., 2009; Ransbotham and Mitra, 2009; Tashi and Ghernaouti-Hélie, 2008)	control development	Security management
security control (Alavi et al., 2016; Ashenden, 2008; Atoum et al., 2014; Azuwa et al., 2017; Bayuk and Mostashari, 2013; Cavusoglu et al., 2004; Collier et al., 2016; Fenz et al., 2013; Goldstein et al., 2011; Hajdarevic and Allen, 2013; Hedström et al., 2011; Hong et al., 2003; Horne et al., 2017; Johnson and Goetz, 2007; Jones and Horowitz, 2012; Knapp et al., 2009; Leon and Saxena, 2010; Lowry and Moody, 2015a; 2015b; Mazur et al., 2015; Narain Singh et al., 2014; Savola, 2007; Savola and Heinonen, 2011; Siponen and Willison, 2009; Sowa and Gabriel, 2009; Sunyaev et al., 2009; Tsiakis and Stephanides, 2005; Young et al., 2016; Zalewski et al., 2014; Zobel and Khansa, 2012)		
control recommendation/implementation (Wood, 1987)		
safeguards (Dzazali et al., 2009; Fenz et al., 2014; Ifinedo, 2012; Liang and Xue, 2009; Tashi and Ghernaouti-Hélie, 2008; Willison and Backhouse, 2006; Yulianto et al., 2016)		
incident response (Abu-Musa, 2010; Alavi et al., 2016; Alqahtani, 2015; Bayuk and Mostashari, 2013; Hajdarevic et al., 2012; Hall et al., 2011; Ifinedo, 2012; Jafari et al., 2010; Jean Camp and Wolfram, 2004; Sowa and Gabriel, 2009; Veiga and Eloff, 2007)	incident management	
incident handling (Johnson and Goetz, 2007; Sharman et al., 2004)		
compromise detection (Boyer and McQueen, 2007; Ransbotham and Mitra, 2009; Savola, 2007)		
breach investigation (Wood, 1987)		
incident management (Mijnhardt et al., 2016; Muthukrishnan and Palaniappan, 2016; Narain Singh et al., 2014; Tran et al., 2016)		
fraud detection (Goldstein et al., 2011; Tran et al., 2016)		
compliance check (Wood, 1987)	monitor and check	
evaluation (measurement) (Azuwa et al., 2017; Gosavi and Bagade, 2015; Pendleton et al., 2017; Savola, 2013; Tu and Yuan, 2014; Wood, 1987; Yaokumah, 2014; Zalewski et al., 2014)		
surveillance (Sharman et al., 2004)		
monitoring (Bayuk and Mostashari, 2013; Mazur et al., 2015; Nazareth and Choi, 2015; Savola, 2013; Sharman et al., 2004)		
auditing (Ashenden, 2008; Atoum et al., 2014; Azuwa et al., 2017; Bayuk and Mostashari, 2013; Jafari et al., 2010; Katos and Adams, 2005; Knapp et al., 2009; Leon and Saxena, 2010; Mishra and Chasalow, 2011; Narain Singh et al., 2014; Ransbotham and Mitra, 2009; Savola, 2009; Sharman et al., 2004; Trèek, 2003; von Solms and von Solms, 2004)		
certification (Savola, 2007; Sowa and Gabriel, 2009; Veiga and Eloff, 2007; von Solms and von Solms, 2004)		
operational processes (Ashenden, 2008; Hayden, 2010; Jafari et al., 2010; Johnson and Goetz, 2007; Sowa and Gabriel, 2009; Trèek, 2003)	operational rules	
administrative security (Kankanhalli et al., 2003; Yeh and Chang, 2007)		
procedures (Boss et al., 2009; Cavusoglu et al., 2004; Dzazali et al., 2009; Hedström et al., 2011; Herath and Rao, 2009; Hong et al., 2003; Karjalainen and Siponen, 2011; Kotulic and Clark, 2004; Merete Hagen et al., 2008; Montesdioca and Maçada, 2015; Osvaldo De Sordi et al., 2014; Tashi and Ghernaouti-Hélie, 2008; Tsiakis and Stephanides, 2005; Veiga and Eloff, 2007)		
processes (Abu-Musa, 2010; Bayuk and Mostashari, 2013; Goel and Chengalur-Smith, 2010; Goldstein et al., 2011; Hajdarevic et al., 2012; Hall et al., 2011; Horne et al., 2017; Kotulic and Clark, 2004; Mazur et al., 2015; Montesdioca and Maçada, 2015; Norman and Yasin, 2013; Purboyo et al., 2011; Ransbotham and Mitra, 2009; Tsiakis and Stephanides, 2005; Vaughn et al., 2003; Yulianto et al., 2016; Zalewski et al., 2014)		
operational readiness(Vaughn et al., 2003)		
process documentation (Sowa and Gabriel, 2009; Yulianto et al., 2016)		
standards (best practices) (Abu-Musa, 2010; Azuwa et al., 2017; Fenz et al., 2013; Goldstein et al., 2011; Hajdarevic and Allen, 2013; Hajdarevic et al., 2012; Knapp et al., 2009; Leon and Saxena, 2010; Mermigas et al., 2013; Mijnhardt et al., 2016; Norman and Yasin, 2013; Smith et al., 2010; Sunyaev et al., 2009; Tu and Yuan, 2014; Uffen and Breitner, 2013; von Solms and von Solms, 2004; Wang et al., 2013; Yulianto et al., 2016)	standards	
ISMS (Azuwa et al., 2017; Hajdarevic and Allen, 2013; Hajdarevic et al., 2012; Herrera, 2005; Mijnhardt et al., 2016; Savola, 2007)		
management implementation (Ernest Chang and Ho, 2006)		
management system (Ashenden, 2008)		
governance (Abu-Musa, 2010; Atoum et al., 2014; Horne et al., 2017; Knapp et al., 2009; Kotulic and Clark, 2004; Norman and Yasin, 2013; von Solms and von Solms, 2004; Yaokumah, 2014)		
communication management (Alavi et al., 2016; AlHogail, 2015; Dhillon and Torkzadeh, 2006; Johnson and Goetz, 2007; Kraemer et al., 2009; Narain Singh et al., 2014; Norman and Yasin, 2013; Smith et al., 2010; Trèek, 2003; Veiga and Eloff, 2007)	communication	
security enforcement (Savola, 2009)		
deterrence (Johnston et al., 2016; Mishra and Chasalow, 2011)		
sanctions (Johnston et al., 2016; Lowry and Moody, 2015b)		
responsibility (Abu-Musa, 2010; Dhillon and Torkzadeh, 2006; Dzazali et al., 2009; Horne et al., 2017; Kraemer et al., 2009; Posey et al., 2015; Sowa and Gabriel, 2009; Wood, 1987)	responsibility	
ownership (AlHogail, 2015; Dhillon and Torkzadeh, 2006; Sharman et al., 2004)		

Table 14
Resources.

First-order code	Second-order code	Cluster
cost (Alavi et al., 2016; Arora et al., 2010; Ben-Aissa et al., 2012; Geer et al., 2003; Hayden, 2010; Ifinedo, 2012; Jafari et al., 2010; Lee and Larsen, 2009; LeMay et al., 2011; Liang and Xue, 2009; Mishra and Chasalow, 2011; Nazareth and Choi, 2015; Tariq, 2012; Tashi and Ghernaouti-Hélie, 2008; Verendel, 2009; Zobel and Khansa, 2012) **cost-benefit/effectiveness** (Cavusoglu et al., 2004; Gonzalez and Sawicka, 2002; Ransbotham and Mitra, 2009; Savola, 2007; Sowa and Gabriel, 2009) **possible cost** (Trèek, 2003) **ROSI** (Alavi et al., 2016; Cavusoglu et al., 2004; Chai et al., 2011; Coronado et al., 2009; Dzazali et al., 2009; Fenz et al., 2013; Gao and Zhong, 2015; Goldstein et al., 2011; Hayden, 2010; Hua and Bapna, 2013; Leon and Saxena, 2010; Lowry and Moody, 2015b; Merete Hagen et al., 2008; Muthukrishnan and Palaniappan, 2016; Nazareth and Choi, 2015; Posey et al., 2015; Pudar et al., 2009; Tashi and Ghernaouti-Hélie, 2008; Tsiakis and Stephanides, 2005; Veiga and Eloff, 2007; Wang et al., 2013; Young et al., 2016)	investment balance	Resources
human resources (Atoum et al., 2014; Dhillon and Torkzadeh, 2006; Kankanhalli et al., 2003; Kraemer et al., 2009; Mijnhardt et al., 2016; Savola, 2007; Soomro et al., 2016; Veiga and Eloff, 2007; Willison and Backhouse, 2006)	human resources	
financial resources (Kankanhalli et al., 2003; Muthukrishnan and Palaniappan, 2016; Sowa and Gabriel, 2009; Tu and Yuan, 2014) **cost control** (Anderson and Moore, 2006) **financial aspect** (Dogaheh, 2010; Ernest Chang and Ho, 2006) **security budget** (Alavi et al., 2016; Beresnevichiene et al., 2010; Horne et al., 2017; Johnson and Goetz, 2007; Kraemer et al., 2009; Lee and Larsen, 2009; Montesdioca and Maçada, 2015; NIST, 2008; Smith et al., 2010; Willison and Backhouse, 2006)	financial resources	
resource support (Abu-Musa, 2010; AlHogail, 2015; Ransbotham and Mitra, 2009; Sowa and Gabriel, 2009; Vaughn et al., 2003; Wilkin and Chenhall, 2010; Zalewski et al., 2014) **economic factors** (Coronado et al., 2009; Fenz et al., 2013; Horne et al., 2017; Hua and Bapna, 2013; Sunyaev et al., 2009; Verendel, 2009) **resource strategy** and value delivery (Yaokumah, 2014)	resource strategy	

References

Abu-Musa, A., 2010. Information security governance in saudi organizations: an empirical study. Inf. Manag. Comput. Secur. 18 (4), 226–276. doi:10.1108/09685221011079180.

AIS Members, 2011. Senior scholars' basket of journals. URL: https://aisnet.org/page/SeniorScholarBasket Last checked: 04.12.2018.

Alavi, R., Islam, S., Mouratidis, H., 2016. An information security risk-driven investment model for analysing human factors. Inf. Comput. Secur. 24 (2), 205–227. doi:10.1108/ICS-01-2016-0006.

AlHogail, A., 2015. Design and validation of information security culture framework. Comput. Human Behav. 49, 567–575. doi:10.1016/j.chb.2015.03.054.

Alqahtani, A., 2015. Towards a framework for the potential cyber-terrorist threat to critical national infrastructure. Inf. Comput. Secur. 23 (5), 532–569. doi:10.1108/ICS-09-2014-0060.

Anderson, R., Moore, T., 2006. The economics of information security. Science (New York, N.Y.) 314, 610–613. doi:10.1126/science.1130992.

Arora, A., Krishnan, R., Telang, R., Yang, Y., 2010. An empirical analysis of software vendors' patch release behavior: impact of vulnerability disclosure. Inf. Syst. Res. 21 (1), 115–132. doi:10.1287/isre.1080.0226.

Ashenden, D., 2008. Information security management: a human challenge? Inf. Secur. Tech. Rep. 13 (4), 195–201. doi:10.1016/j.istr.2008.10.006.

Atoum, I., Otoom, A., Abu Ali, A., 2014. A holistic cyber security implementation framework. Inf. Manag. Comput. Secur. 22 (3), 251–264. doi:10.1108/IMCS-02-2013-0014.

Azuwa, M.P., Sahib, S., Shamsuddin, S., 2017. Technical security metrics model in compliance with iso/iec 27001 standard. Int. J. Cyber-Secur. Digital Forens. (IJCSDF) 1 (4), 280–288.

Bayuk, J., Mostashari, A., 2013. Measuring systems security. Syst. Eng. 16 (1), 1–14. doi:10.1002/sys.21211.

Bayuk, J.L., 2013. Security as a theoretical attribute construct. Comput. Secur. 37, 155–175. doi:10.1016/j.cose.2013.03.006.

Ben-Aissa, A., Abercrombie, R.K., Sheldon, F.T., Mili, A., 2012. Defining and computing a value based cyber-security measure. Inf. Syst. e-Business Manag. 10 (4), 433–453. doi:10.1007/s10257-011-0177-1.

Beresnevichiene, Y., Pym, D., Shiu, S., 2010. Decision support for systems security investment. In: 2010 IEEE/IFIP Network Operations and Management Symposium workshops, pp. 118–125. doi:10.1109/NOMSW.2010.5486590.

Bernard, T. S., Cowley, S., 2017. Equifax breach caused by lone employee's error, former c.e.o. says. URL: https://www.nytimes.com/2017/10/03/business/equifax-congress-data-breach:html, Last checked: 01.12.2018.

Björck, F., Henkel, M., Stirna, J., Zdravkovic, J., 2015. Cyber resilience – fundamentals for a definition. In: Rocha, A., Correia, A.M., Costanzo, S., Reis, L.P. (Eds.), New Contributions in Information Systems and Technologies. In: Advances in Intelligent Systems and Computing, 353. Springer International Publishing, Cham, pp. 311–316. doi:10.1007/978-3-319-16486-1_31.

Boehm, J., Merrath, P., Poppensieker, T., Riemenschnitter, R., Stähle, T., 2017. Cyber risk measurement and the holistic cybersecurity approach. URL: https://www.mckinsey.com/business-functions/risk/our-insights/cyber-risk-measurement-and-the-holistic-cybersecurity-approach Last checked: 03.12.2018.

Bogner, A., Littig, B., Menz, W., 2014. Interviews mit Experten: Eine praxisorientierte Einführung. Qualitative Sozialforschung. Springer Fachmedien Wiesbaden.

Bortz, J., Döring, N., 1995. Forschungsmethoden und Evaluation. Springer-Lehrbuch, Springer Berlin Heidelberg.

Boss, S.R., Kirsch, L.J., Angermeier, I., Shingler, R.A., Boss, R.W., 2009. If someone is watching, i'll do what i'm asked: Mandatoriness, control, and information security. Eur. J. Inf. Syst. 18 (2), 151–164. doi:10.1057/ejis.2009.8.

Boyer, W., McQueen, M., 2007. Ideal based cyber security technical metrics for control systems. In: Critical information infrastructures security, pp. 246–260. doi:10.1007/978-3-540-89173-421.

Cavusoglu, H., Mishra, B., Raghunathan, S., 2004. A model for evaluating it security investments. Commun. ACM 47 (7), 87–92. doi:10.1145/1005817.1005828.

Chai, S., Kim, M., Rao, H.R., 2011. Firms' information security investment decisions: Stock market evidence of investors' behavior. Decis. Support Syst. 50 (4), 651–661. doi:10.1016/j.dss.2010.08.017.

Cisco Systems Inc., 2018. Cisco 2018: annual cybersecurity report. Technical Report. Cisco Systems Inc.

Collier, Z.A., Panwar, M., Ganin, A.A., Kott, A., Linkov, I., 2016. Security metrics in industrial control systems. In: Colbert, E.J.M., Kott, A. (Eds.), Cyber-Security of SCADA and Other Industrial Control Systems. In: Advances in Information Security. Springer, Switzerland, pp. 167–185. doi:10.1007/978-3-319-32125-7_9.

Corbin, J., Strauss, A., 1990. Grounded theory research: procedures, canons and evaluative criteria. Zeitschrift für Soziologie 19 (6), 418–427 doi:10.1515/zfsoz-1990-0602.

Coronado, A.S., Mahmood, M.A., Pahnila, S., Luciano, E.M., 2009. Measuring effectiveness of information systems security: an empirical research. In: 15th Americas Conference on Information Systems, pp. 282–290.

Crossler, R., Belanger, F., 2012. The quest for complete security protection: an empirical analysis of an individual's 360 degree protection from file and data loss. In: 18th Americas Conference on Information Systems, pp. 1–6.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., Baskerville, R., 2013. Future directions for behavioral information security research. Comput. Secur. 32, 90–101. doi:10.1016/j.cose.2012.09.010.

DeLone, W.H., McLean, E.R., 1992. Information systems success: the quest for the dependent variable. Inf. Syst. Res. 3 (1), 60–95. doi:10.1287/isre.3.1.60.

Dhillon, G., Torkzadeh, G., 2006. Value-focused assessment of information system security in organizations. Inf. Syst. J. 16 (3), 293–314. doi:10.1111/j.1365-2575.2006.00219.x.

Diesch, R., Pfaff, M., Krcmar, H., 2018. Prerequisite to measure information security: a state of the art literature review. In: 4th International Conference on

Information Systems Security and Privacy (ICISSP), pp. 207–215. doi:10.5220/0006545602070215.

Dinev, T., Goo, J., Hu, Q., Nam, K., 2009. User behaviour towards protective information technologies: the role of national cultural differences. Inf. Syst. J. 19 (4), 391–412. doi:10.1111/j.1365-2575.2007.00289.x.

Dinev, T., Hu, Q., 2007. The centrality of awareness in the formation of user behavioral intention toward protective information technologies. J. Assoc. Inf. Syst. 8 (7), 386–408.

Dogaheh, M.A., 2010. Introducing a framework for security measurements. In: IEEE International Conference on Information Theory and Information Security, pp. 638–641. doi:10.1109/ICITIS.2010.5689505.

Dzazali, S., Sulaiman, A., Zolait, A.H., 2009. Information security landscape and maturity level: case study of malaysian public service (mps) organizations. Gov. Inf. Q. 26 (4), 584–593. doi:10.1016/j.giq.2009.04.004.

Ernest Chang, S., Ho, C.B., 2006. Organizational factors to the effectiveness of implementing information security management. Indus. Manag. Data Syst. 106 (3), 345–361. doi:10.1108/02635570610653498.

Fenz, S., Heurix, J., Neubauer, T., Pechstein, F., 2014. Current challenges in information security risk management. Inf. Manag. Comput. Secur. 22 (5), 410–430. doi:10.1108/IMCS-07-2013-0053.

Fenz, S., Neubauer, T., Accorsi, R., Koslowski, T., 2013. Forisk: formalizing information security risk and compliance management. In: 43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop, pp. 1–4. doi:10.1109/DSNW.2013.6615533.

Gao, X., Zhong, W., 2015. Information security investment for competitive firms with hacker behavior and security requirements. Annal. Oper. Res. 235 (1), 277–300. doi:10.1007/s10479-015-1925-2.

Geer, D., Hoo, K.S., Jaquith, A., 2003. Information security: why the future belongs to the quants. IEEE Secur. Privacy Mag. 1 (4), 24–32. doi:10.1109/MSECP.2003.1219053.

Glaser, B.G., Strauss, A.L., 1967. The discovery of grounded theory: strategies for qualitative research. AldineTransaction, New Brunswick.

Goel, S., Chengalur-Smith, I.N., 2010. Metrics for characterizing the form of security policies. J. Strategic Inf. Syst. 19 (4), 281–295. doi:10.1016/j.jsis.2010.10.002.

Goldstein, J., Chernobai, A., Benaroch, M., 2011. An event study analysis of the economic impact of it operational risk and its subcategories. J. Assoc. Inf. Syst. 11 (9), 606–631.

Gonzalez, J.J., Sawicka, A., 2002. A framework for human factors in information security. In: 2002 WSEAS International Conference on Information Security, Hardware/Software Codesign, E-Commerce and Computer Networks, pp. 1871–1877.

Gosavi, H.R., Bagade, A.M., 2015. A review on zero day attack safety using different scenarios. Eur. J. Adv. Eng. Technol. 2 (1), 30–34.

Gupta, A., Hammond, R., 2005. Information systems security issues and decisions for small businesses. Inf. Manag. Comput. Secur. 13 (4), 297–310. doi:10.1108/09685220510614425.

Hajdarevic, K., Allen, P., 2013. A new method for the identification of proactive information security management system metrics. In: 36th International Convention on Information & Communication Technology, Electronics & Microelectronics, pp. 1121–1126.

Hajdarevic, K., Pattinson, C., Kozaric, K., Hadzic, A., 2012. Information security measurement infrastructure for kpi visualization. In: Proceedings of the 35th International Convention MIPRO, pp. 1543–1548.

Hall, J.H., Sarkani, S., Mazzuchi, T.A., 2011. Impacts of organizational capabilities in information security. Inf. Manag. Comput. Secur. 19 (3), 155–176. doi:10.1108/09685221111153546.

Hayden, L., 2010. IT security metrics: a practical framework for measuring security & protecting data. McGraw Hill, New York.

Hedström, K., Kolkowska, E., Karlsson, F., Allen, J.P., 2011. Value conflicts for information security management. J. Strateg. Inf. Syst. 20 (4), 373–384. doi:10.1016/j.jsis.2011.06.001.

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., Rao, H.R., 2014. Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service. Inf. Syst. J. 24 (1), 61–84. doi:10.1111/j.1365-2575.2012.00420.x.

Herath, T., Rao, H.R., 2009. Protection motivation and deterrence: a framework for security policy compliance in organisations. Eur. J. Inf. Syst. 18 (2), 106–125. doi:10.1057/ejis.2009.6.

Herrera, S., 2005. Information security management metrics development. In: 39th Annual 2005 International Carnahan Conference on Security Technology, pp. 51–56. doi:10.1109/CCST.2005.1594818.

Herzog, A., Shahmehri, N., Duma, C., 2007. An ontology of information security. Int. J. Inf. Secur. Privacy 1 (4), 1–23. doi:10.4018/jisp.2007100101.

Holm, H., Afridi, K.K., 2015. An expert-based investigation of the common vulnerability scoring system. Comput. Secur. 53, 18–30. doi:10.1016/j.cose.2015.04.012.

Höne, K., Eloff, J., 2002. Information security policy — what do international information security standards say? Comput. Secur. 21 (5), 402–409. doi:10.1016/S0167-4048(02)00504-7.

Hong, K.-S., Chi, Y.-P., Chao, L.R., Tang, J.-H., 2003. An integrated system theory of information security management. Inf. Manag. Comput. Secur. 11 (5), 243–248. doi:10.1108/09685220310500153.

Horne, C.A., Maynard, S.B., Ahmad, A., 2017. Information security strategy in organisations: review, discussion and future research. Aust. J. Inf. Syst. 21. doi:10.3127/ajis.v21i0.1427.

Hu, Q., Dinev, T., Hart, P., Cooke, D., 2012. Managing employee compliance with information security policies: the critical role of top management and organizational culture. Decis. Sci. 43 (4), 615–660. doi:10.1111/j.1540-5915.2012.00361.x.

Hua, J., Bapna, S., 2013. The economic impact of cyber terrorism. J. Strateg. Inf. Syst. 22 (2), 175–186. doi:10.1016/j.jsis.2012.10.004.

Idika, N., Bhargava, B., 2012. Extending attack graph-based security metrics and aggregating their application. IEEE Trans. Depend. Secure Comput. 9 (1), 75–85. doi:10.1109/TDSC.2010.61.

Ifinedo, P., 2012. Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. Comput. Secur. 31 (1), 83–95. doi:10.1016/j.cose.2011.10.007.

ISACA, 2012. COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. ISACA.

ISF, 2018. Standard of good practice for information security. Technical Report. Information Security Forum Limited. (ISF).

ISO/IEC, 2018. ISO/IEC 27000:2018(E): Information technology - Security techniques - Information security management systems - Overview and vocabulary. Standard. ISO/IEC, Switzerland.

Jafari, S., Mtenzi, F., Fitzpatrick, R., O'Shea, B., 2010. Security metrics for e-healthcare information systems: a domain specific metrics approach. Int. J. Digital Soc. (IJDS) 1 (4), 238–245.

Jean Camp, L., Wolfram, C., 2004. Pricing security: vulnerabilities as externalities. Econ. Inf. Secur. 12, 17–34. doi:10.1007/1-4020-8090-5_2.

Joh, H., Malaiya, Y.K., 2011. Defining and assessing quantitative security risk measures using vulnerability lifecycle and cvss metrics. In: The 2011 International Conference on Security and Management, pp. 10–16.

Johnson, M.E., Goetz, E., 2007. Embedding information security into the organization. IEEE Secur. Privacy Mag. 5 (3), 16–24. doi:10.1109/MSP.2007.59.

Johnston, A.C., Warkentin, M., McBride, M., Carter, L., 2016. Dispositional and situational factors: influences on information security policy violations. Eur. J. Inf. Syst. 25 (3), 231–251. doi:10.1057/ejis.2015.15.

Jones, R.A., Horowitz, B., 2012. A system-aware cyber security architecture. Syst. Eng. 15 (2), 225–240. doi:10.1002/sys.21206.

Kankanhalli, A., Teo, H.-H., Tan, B.C., Wei, K.-K., 2003. An integrative study of information systems security effectiveness. Int. J. Inf. Manag. 23 (2), 139–154. doi:10.1016/S0268-4012(02)00105-6.

Karjalainen, M., Siponen, M., 2011. Toward a new meta-theory for designing information systems (is) security training approaches. J. Assoc. Inf. Syst. 12 (8), 518–555.

Katos, V., Adams, C., 2005. Modelling corporate wireless security and privacy. J. Strateg. Inf. Syst. 14 (3), 307–321. doi:10.1016/j.jsis.2005.07.006.

Knapp, K., Marshall, T., Rainer, R.K., Morrow, D., 2006. The top information security issues facing organizations: what can government do to help? Inf. Syst. Secur. 15 (4), 51–58. doi:10.1201/1086.1065898X/46353.15.4.20060901/95124.6.

Knapp, K.J., Franklin Morris, R., Marshall, T.E., Byrd, T.A., 2009. Information security policy: an organizational-level process model. Comput. Secur. 28 (7), 493–508. doi:10.1016/j.cose.2009.07.001.

Kotenko, I., Bogdanov, V., 2009. Proactive monitoring of security policy accomplishment in computer networks. In: Proceedings of the 5th IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems, Technology and Applications, pp. 364–369. doi:10.1109/IDAACS.2009.5342961.

Kotulic, A.G., Clark, J.G., 2004. Why there aren't more information security research studies. Inf. Manag. 41 (5), 597–607. doi:10.1016/j.im.2003.08.001.

Kraemer, S., Carayon, P., Clem, J., 2009. Human and organizational factors in computer and information security: pathways to vulnerabilities. Comput. Secur. 28 (7), 509–520. doi:10.1016/j.cose.2009.04.006.

Kumar, R.L., Park, S., Subramaniam, C., 2008. Understanding the value of countermeasure portfolios in information systems security. J. Manag. Inf. Syst. 25 (2), 241–280. doi:10.2753/MIS0742-1222250210.

Lee, C.H., Geng, X., Raghunathan, S., 2016. Mandatory standards and organizational information security. Inf. Syst. Res. 27 (1), 70–86. doi:10.1287/isre.2015.0607.

Lee, Y., Larsen, K.R., 2009. Threat or coping appraisal: determinants of smb executives' decision to adopt anti-malware software. Eur. J. Inf. Syst. 18 (2), 177–187. doi:10.1057/ejis.2009.11.

LeMay, E., Ford, M.D., Keefe, K., Sanders, W.H., Muehrcke, C., 2011. Model-based security metrics using adversary view security evaluation (advise). In: Eighth International Conference on Quantitative Evaluation of SysTems, pp. 191–200. doi:10.1109/QEST.2011.34.

Leon, P.G., Saxena, A., 2010. An approach to quantitatively measure information security. In: 3rd India Software Engineering Conference.

Liang, H., Xue, Y., 2009. Avoidance of information technology threats: a theoretical perspective. MIS Q. 33 (1), 71–90.

Lowry, P.B., Moody, G.D., 2015. Proposing the control-reactance compliance model (crcm) to explain opposing motivations to comply with organisational information security policies. Inf. Syst. J. 25 (5), 433–463. doi:10.1111/isj.12043.

Lowry, P.B., Moody, G.D., 2015. Proposing the control-reactance compliance model (crcm) to explain opposing motivations to comply with organisational information security policies. Inf. Syst. J. 25 (5), 433–463. doi:10.1111/isj.12043.

Manhart, M., Thalmann, S., 2015. Protecting organizational knowledge: a structured literature review. J. Know. Manag. 19 (2), 190–211. doi:10.1108/JKM-05-2014-0198.

May, T.A., 1997. The death of roi: re–thinking it value measurement. Inf. Manag. Comput. Secur. 5 (3), 90–92. doi:10.1108/09685229710175756.

Mayring, P., 2015. Qualitative Inhaltsanalyse: Grundlagen und Techniken. Beltz Pädagogik. Beltz.

Mazur, K., Ksiezopolski, B., Kotulski, Z., 2015. The robust measurement method for security metrics generation. Comput. J. 58 (10), 2280–2296. doi:10.1093/comjnl/bxu100.

Merete Hagen, J., Albrechtsen, E., Hovden, J., 2008. Implementation and effectiveness of organizational information security measures. Inf. Manag. Comput. Secur. 16 (4), 377–397. doi:10.1108/09685220810908796.

Mermigas, D., Patsakis, C., Pirounias, S., 2013. Quantification of information systems security with stochastic calculus. In: Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop, pp. 1–9. doi:10.1145/2459976.2460030.

Mijnhardt, F., Baars, T., Spruit, M., 2016. Organizational characteristics influencing sme information security maturity. J. Comput. Inf. Syst. 56 (2), 106–115. doi:10.1080/08874417.2016.1117369.

Mishra, S., Chasalow, L., 2011. Information security effectiveness: a research framework. Iss. Inf. Syst. 7 (1), 246–255.

Montesdioca, G.P.Z., Maçada, A.C.G., 2015. Measuring user satisfaction with information security practices. Comput. Secur. 48, 267–280. doi:10.1016/j.cose.2014.10.015.

Muthukrishnan, S.M., Palaniappan, S., 2016. Security metrics maturity model for operational security. In: IEEE Symposium on Computer Applications and Industrial Electronics, pp. 101–106. doi:10.1109/ISCAIE.2016.7575045.

Narain Singh, A., Gupta, M.P., Ojha, A., 2014. Identifying factors of "organizational information security management". J. Enterp. Inf. Manag. 27 (5), 644–667. doi:10.1108/JEIM-07-2013-0052.

Nazareth, D.L., Choi, J., 2015. A system dynamics model for information security management. Inf. Manag. 52 (1), 123–134. doi:10.1016/j.im.2014.10.009.

NIST, 2008. NIST SP 800-55r1: performance measurement guide for information security. Technical Report. National Institute of Standards and Technology.

NIST, 2013. NISTIR 7298r2: glossary of key information security terms. Technical Report. National Institute of Standards and Technology.

NIST, 2015. NIST SP 800-30r1: risk management guide for information technology systems. Technical Report. National Institute of Standards and Technology.

NIST, 2018. NIST SP 800-37r2: risk management framework for information systems and organizations. Technical Report. National Institute of Standards and Technology.

NIST, 2018b. Nist special publication 800-series general information. URL: https://www.nist.gov/itl/nist-special-publication-800-series-general-information Last checked: 07.05.2019.

Norman, A.A., Yasin, N.M., 2013. Information systems security management (issm) success factor: retrospection from the scholars. African J. Bus. Manag. 7 (27), 2646–2656. doi:10.5897/AJBM11.2479.

Osvaldo De Sordi, J., Meireles, M., Carvalho de Azevedo, M., 2014. Information selection by managers: priorities and values attributed to the dimensions of information. Online Inf. Rev. 38 (5), 661–679. doi:10.1108/OIR-01-2014-0006.

Pendleton, M., Garcia-Lebron, R., Cho, J.-H., Xu, S., 2017. A survey on systems security metrics. ACM Comput. Surv. 49 (4), 1–35. doi:10.1145/3005714.

Ponemon Institute LLC, 2018. 2018 cost of a data breach study: global overview. Technical Report. Ponemon Institute LLC.

Posey, C., Roberts, T.L., Lowry, P.B., 2015. The impact of organizational commitment on insiders' motivation to protect organizational information assets. J. Manag. Inf. Syst. 32 (4), 179–214. doi:10.1080/07421222.2015.1138374.

Premaratne, U., Samarabandu, J., Sidhu, T., Beresh, B., Tan, J.-C., 2008. Application of security metrics in auditing computer network security: acase study. In: 4th International Conference on Information and Automation for Sustainability, pp. 200–205. doi:10.1109/ICIAFS.2008.4783996.

Pudar, S., Manimaran, G., Liu, C.-C., 2009. Penet: a practical method and tool for integrated modeling of security attacks and countermeasures. Comput. Secur. 28 (8), 754–771. doi:10.1016/j.cose.2009.05.007.

Purboyo, T.W., Rahardjo, B., Kuspriyanto, 2011. Security metrics: a brief survey. In: 2011 2nd International Conference on Instrumentation, Communications, Information Technology and Biomedical Engineering, pp. 79–82. doi:10.1109/ICICI-BME.2011.6108598.

Ransbotham, S., Mitra, S., 2009. Choice and chance: a conceptual model of paths to information security compromise. Inf. Syst. Res. 20 (1), 121–139. doi:10.1287/isre.1080.0174.

Savola, R., 2007. Towards a security metrics taxonomy for the information and communication technology industry. In: International Conference on Software Engineering Advances (ICSEA), p. 60. doi:10.1109/ICSEA.2007.79.

Savola, R.M., 2009. A security metrics taxonomization model for software-intensive systems. J. Inf. Process. Syst. 5 (4), 197–206. doi:10.3745/JIPS.2009.5.4.197.

Savola, R.M., 2013. Quality of security metrics and measurements. Comput. Secur. 37, 78–90. doi:10.1016/j.cose.2013.05.002.

Savola, R.M., Heinonen, P., 2011. A visualization and modeling tool for security metrics and measurements management. In: 2011 Information Security for South Africa, pp. 1–8. doi:10.1109/ISSA.2011.6027518.

Sharman, R., Rao, R., Upadhyaya, S., 2004. Metrics for information security: a literature review. In: 10th Americas Conference on Information Systems, pp. 1437–1440.

Silic, M., Back, A., 2014. Information security: critical review and future directions for research. Inf. Manag. Comput. Secur. 22 (3), 279–308. doi:10.1108/IMCS-05-2013-0041.

Siponen, M., Willison, R., 2009. Information security management standards: problems and solutions. Inf. Manag. 46 (5), 267–270. doi:10.1016/j.im.2008.12.007.

SJR, 2018. Sjr: Scientific journal rankings. URL: https://www.scimagojr.com/journalrank.php Last checked: 04.12.2018.

Smith, S., Winchester, D., Bunker, D., Jaimeson, R., 2010. Circuits of power: a study of mandated compliance to an information systems security de jure standard in a government organization. MIS Q. 34 (3), 463–486.

Soomro, Z.A., Shah, M.H., Ahmed, J., 2016. Information security management needs more holistic approach: a literature review. Int. J. Inf. Manag. 36 (2), 215–225. doi:10.1016/j.ijinfomgt.2015.11.009.

Sowa, S., Gabriel, R., 2009. Multidimensional management of information security: a metrics based approach merging business and information security topics. In: International Conference on Availability, Reliability and Security. IEEE, pp. 750–755. doi:10.1109/ARES.2009.26.

Straub, D.W., Welke, R.J., 1998. Coping with systems risk: security planning models for management decision making. MIS Q. 22 (4), 441. doi:10.2307/249551.

Sunyaev, A., Tremmel, F., Mauro, C., LeimeisterJ. M. & Krcmar, H., 2009. A re-classification of is security analysis approaches. In: 15th Americas Conference on Information Systems, pp. 1–10.

Tanna, G.B., Gupta, M., Rao, H.R., Upadhyaya, S., 2005. Information assurance metric development framework for electronic bill presentment and payment systems using transaction and workflow analysis. Decis. Support Syst. 41 (1), 242–261. doi:10.1016/j.dss.2004.06.013.

Tariq, M.I., 2012. Towards information security metrics framework for cloud computing. Int. J. Cloud Comput. Serv. Sci. (IJ-CLOSER) 1 (4). doi:10.11591/closer.v1i4.1442.

Tashi, I., Ghernaouti-Hélie, S., 2008. Efficient security measurements and metrics for risk assessment. In: The Third International Conference on Internet Monitoring and Protection, pp. 131–138. doi:10.1109/ICIMP.2008.34.

Thycopic Software Ltd., 2017. The 2017 state of cybersecurity metrics annual report. Technical Report. Thycopic Software Ltd.

Tran, H., Campos-Nanez, E., Fomin, P., Wasek, J., 2016. Cyber resilience recovery model to combat zero-day malware attacks. Comput. Secur. 61, 19–31. doi:10.1016/j.cose.2016.05.001.

Trèek, D., 2003. An integral framework for information systems security management. Comput. Secur. 22 (4), 337–360. doi:10.1016/S0167-4048(03)00413-9.

Tsiakis, T., Stephanides, G., 2005. The economic approach of information security. Comput. Secur. 24 (2), 105–108. doi:10.1016/j.cose.2005.02.001.

Tu, C.Z., Yuan, Y., Archer, N., Connelly, C.E., 2018. Strategic value alignment for information security management: a critical success factor analysis. Inf. Comput. Secur. 26 (2), 150–170. doi:10.1108/ICS-06-2017-0042.

Tu, Z., Yuan, Y., 2014. Critical success factors analysis on effective information security management: a literature review. In: 20th Americas Conference on Information Systems, pp. 1874–1886.

Uffen, J., Breitner, M.H., 2013. Management of technical security measures: an empirical examination of personality traits and behavioral intentions. In: 46th Hawaii International Conference on System Sciences, pp. 4551–4560. doi:10.1109/HICSS.2013.388.

Vance, A., Eargle, D., Anderson, B.B., Kirwan, C.B., 2014. Using measures of risk perception to predict information security behavior: insights from electroencephalography (eeg). J. Assoc. Inf. Syst. 15, 679–722.

Vaughn, R.B., Henning, R., Siraj, A., 2003. Information assurance measures and metrics - state of practice and proposed taxonomy. In: Proceedings of the 36th Annual Hawaii International Conference on System Sciences doi:10.1109/HICSS.2003.1174904.

Veiga, A.D., Eloff, J.H.P., 2007. An information security governance framework. Inf. Syst. Manag. 24 (4), 361–372. doi:10.1080/10580530701586136.

Velki, T., Solic, K., Ocevcic, H., 2014. Development of users' information security awareness questionnaire (uisaq) – ongoing work. In: 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp. 1417–1421. doi:10.1109/MIPRO.2014.6859789.

Verendel, V., 2009. Quantified security is a weak hypothesis: a critical survey of results and assumptions. In: Proceedings of the 2009 workshop on New security paradigms workshop, pp. 37–50. doi:10.1145/1719030.1719036.

von Solms, B., von Solms, R., 2004. The 10 deadly sins of information security management. Comput. Secur. 23 (5), 371–376. doi:10.1016/j.cose.2004.05.002.

von Solms, R., van der Haar, H., von Solms, S.H., Caelli, W.J., 1994. A framework for information security evaluation. Inf. Manag. 26 (3), 143–153. doi:10.1016/0378-7206(94)90038-8.

von Solms, R., van Niekerk, J., 2013. From information security to cyber security. Comput. Secur. 38, 97–102. doi:10.1016/j.cose.2013.04.004.

Wang, C., Wulf, W.A., 1997. Towards a framework for security measurement. In: 20th National Information Systems Security Conference, pp. 522–533.

Wang, T., Kannan, K.N., Ulmer, J.R., 2013. The association between the disclosure and the realization of information security risk factors. Inf. Syst. Res. 24 (2), 201–218. doi:10.1287/isre.1120.0437.

Webster, J., Watson, R.T., 2002. Analyzing the past to prepare for the future: writing a literature review. MIS Q. 26 (2), xiii–xxiii.

Wilkin, C.L., Chenhall, R.H., 2010. A review of it governance: a taxonomy to inform accounting information systems. J. Inf. Syst. 24 (2), 107–146. doi:10.2308/jis.2010.24.2.107.

Willison, R., Backhouse, J., 2006. Opportunities for computer crime: considering systems risk from a criminological perspective. Eur. J. Inf. Syst. 15 (4), 403–414. doi:10.1057/palgrave.ejis.3000592.

Wolfswinkel, J.F., Furtmueller, E., Wilderom, C.P.M., 2013. Using grounded theory as a method for rigorously reviewing literature. Eur. J. Inf. Syst. 22 (1), 45–55. doi:10.1057/ejis.2011.51.

Wood, C.C., 1987. Information systems security: management success factors. Comput. Secur. 6 (4), 314–320. doi:10.1016/0167-4048(87)90066-6.

Yaokumah, W., 2014. Information security governance implementation within ghanaian industry sectors. Inf. Manag. Comput. Secur. 22 (3), 235–250. doi:10.1108/IMCS-06-2013-0044.

Yeh, Q.-J., Chang, A.J.-T., 2007. Threats and countermeasures for information system security: a cross-industry study. Inf. Manag. 44 (5), 480–491. doi:10.1016/j.im.2007.05.003.

Young, D., Lopez, J., Rice, M., Ramsey, B., McTasney, R., 2016. A framework for incorporating insurance in critical infrastructure cyber risk strategies. Int. J. Crit. Infrastruct. Protect. 14, 43–57. doi:10.1016/j.ijcip.2016.04.001.

Yulianto, S., Lim, C., Soewito, B., 2016. Information security maturity model: a best practice driven approach to pci dss compliance. In: 2016 IEEE Region 10 Symposium, pp. 65–70. doi:10.1109/TENCONSpring.2016.7519379.

Zalewski, J., Drager, S., McKeever, W., Kornecki, A.J., 2014. Measuring security: a challenge for the generation. In: 2014 Federated Conference on Computer Science and Information Systems, pp. 131–140. doi:10.15439/2014F490.

Zobel, C.W., Khansa, L., 2012. Quantifying cyberinfrastructure resilience against multi-event attacks. Decis. Sci. 43 (4), 687–710. doi:10.1111/j.1540-5915.2012.00364.x.

Rainer Diesch received the degree of M.Sc. from the Ludwig-Maximilians-University of Munich, 2016. At present, he is a member of a research team at the fortiss GmbH, an affiliated institute of the Technical University of Munich. Rainer Diesch is currently doing his Ph.D. in Business Informatics at the Technical University of Munich on the Cair of Information Systems. His research interest includes information security management, security measurement and information management.

Matthias Pfaff received his PhD degree (Dr. rer nat.) in 2018 from the Technical University of Munich in the topic of semantic data integration. He previously studied computer science at the Goethe University Frankfurt (degree Dipl.-Inf). Since 2011 he is working at fortiss, he heads the competence field æbusiness model & service engineeringg (BM&SE) and is responsible for the fortiss Application Center for AI. His research interests include semantic technologies for data integration and ontologies especially for business applications.

Helmut Krcmar studied business management in Saarbrÿucken and obtained his doctorate in 1983. He worked as a postdoctoral fellow at the IBM Los Angeles Scientific Center and as assistant professor of information systems at the New York University and the City University of New York. Since 2002 he holds the Chair for Information Systems at the Technical University of Munich. From 2010 to 2013, he served as Dean of the Faculty of Computer Science.

SoK: Linking Information Security Metrics to Management Success Factors

Rainer Diesch
diesch@fortiss.org
fortiss GmbH
Munich, Germany

Helmut Krcmar
helmut.krcmar@tum.de
Technical University of Munich
Garching, Germany

ABSTRACT

Information security metrics are used to measure the effectiveness of information security countermeasures. A large number of metrics and their technical nature creates difficulties when generating reports for the information security management level of an organization. Managers struggle with the usefulness and clarity of the metrics because they are not linked to the security management goals. Also, responsible managers with no technical information security background struggle to understand the metrics. Therefore, this study uses a state-of-the-art literature analysis together with the Goal-Question-Metric approach to investigate linking technical security metrics to management success factors. This study enables the management to design appropriate security reports for their organization and to direct the metrics toward making goal-oriented decisions. Furthermore, the study invites future research by revealing areas in which security metrics do not exist and create new solutions and studies to suggest a standardized information security dashboard.

CCS CONCEPTS

• **General and reference** → **Measurement**; **Metrics**; • **Computer systems organization** → *Maintainability and maintenance*; • **Security and privacy** → **Logic and verification**; *Vulnerability management*.

KEYWORDS

information security metrics, security management success factors, goal-question-metric approach, systematic literature review

ACM Reference Format:
Rainer Diesch and Helmut Krcmar. 2020. SoK: Linking Information Security Metrics to Management Success Factors. In *The 15th International Conference on Availability, Reliability and Security (ARES 2020), August 25–28, 2020, Virtual Event, Ireland*. ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3407023.3407059

1 INTRODUCTION

Information security is one of an organization‘s most important issues. If an organization does not deal with information security, the repercussions affect not only finances but also the firm‘s reputation and legal standing [51]. Therefore, various standards and best practices like the ISO/IEC 27000 series, the NIST 800 series or other national and international frameworks like COBIT or ITIL have been put in place. These standards all deal with metrics and measurements for the implementation and further improvement of the information security management within organizations.

An information security assessment is one of the most important activities conducted by information security management and technical information security employees. Audits or security metrics are the methods used to assess an organization‘s information security status. Because information security can not be measured directly [56], multiple measures will be needed in order to quantify aspects of the complex information security construct [52]. Therefore, most of the standards and best practices currently in place describe multiple metrics needed to quantify certain aspects of information security. These standards and best practices include the ISO/IEC 27000 series with the ISO/IEC 27004 document [29] and the NIST 800 series with the special publication NIST SP 800-55r1 [36] to mention only two.

These standards have different areas of focus. While the ISO/IEC 27000 covers the information security management perspective, the NIST 800 series deals with a more technical view. The different perspectives are derived from the shift in responsibility from the technical information security employees to management [20]. Management has other questions than technical employees have. These include questions like whether the security is better this year, what management is getting for their security dollars or even how to compare their security to that of their peers [24]. These questions must be answered not only by information security experts who have become managers but also by managers with less security knowledge. These managers are often located in small- and medium-sized businesses and came from other areas of expertise. Now they have to deal with issues involving complex information security and be responsible for it. To answer the management questions, rigorous metrics need to be defined and linked to the organization‘s management goals in order to support management decisions.

There are various information security metrics and frameworks in place for management. However, there is a gap in the connection between the technical security metrics and managements goals. Information security managers tend to develop metrics with a top-down approach based on international standards, but they do not consider the realities of daily work [26]. Also, many security managers make decisions based on their experience, judgment and best knowledge. The reason for this is that managers do not have effective metrics in place, that security is complex and sensitive, and

ARES 2020, August 25–28, 2020, Virtual Event, Ireland

ACM ISBN 978-1-4503-8833-7/20/08…$15.00
https://doi.org/10.1145/3407023.3407059

managers sometimes do not have enough historical data [14]. Recent research articles have mentioned the gap that exists because of security metrics that are not connected to existing information security models or are not aligned to the management goals and strategic objectives of information security management [4, 6, 17, 19, 38].

This paper investigates the question of how information security metrics characterize and quantifies certain aspects of management success factors in the information security area. For this purpose, a literature analysis was conducted to obtain information security metrics. The next step was to use 12 management success factors [20] as goals to conduct a Goal-Question-Metric approach in conjunction with the previously obtained information security metrics. This methodology was suggested by Rudolph and Schwarz [42] which also stated the given gap and conclude, that this should "lead to a more goal-oriented strategy for deriving metrics that answers relevant questions and met predefined security goals". The result is a list of metrics organized in clusters by questions and overall information security management goals. To the best knowledge of the authors, this is the first time information security metrics and information security management goals have been mapped this way. This research also includes a detailed description of what these metrics measure from the management perspective.

The remainder of this paper is structured as follows. Section 2 discusses the background and related work as well as the prerequisites for this paper. Section 3 outlines the methodology used to obtain the results. The results with the clustered information security metrics, the linkage to the management goals and a detailed description is given in section 4. Section 5 critically discusses the results and contains suggestions for future research. The paper closes with a conclusion of the entirety of the work in section 6.

2 BACKGROUND AND RELATED WORK

A discussion of the link between information security metrics and the information security management goals includes the background of both worlds. Thus, section 2.1 outlines the information security metrics with their different research areas and their focus in the past. Also, a definition of the terms is given within this section. In section 2.2, an introduction to the current standards and best practices in information security management is included along with management success factors defined in the literature.

2.1 Information Security Metrics

The terms metric and measure are mostly used as synonyms in both practice and the literature. Also, the term metric does have different definitions depending on the subject area, the authors' preference, or the context in which they are being used. Azuwa et al. [4] reveals six different definitions of the term metric and measurement. This work differentiates the meaning of metrics and the measurement according to Pendleton et al. [38]. The authors noted that *"metric refers to assigning a value to an object while measurement is the process of estimating attributes of an object"* [38]. In order to clarify the meaning of metrics, the following definition by Verendel [53] is used in this research: *"A metric assigns data onto some kind of scale in order to correctly represent some security attribute of a system under consideration"* [53].

Information security metrics are well discussed in existing research. Articles deal with the development of metrics [17, 35, 55, 56], taxonomies [38, 39, 52], usefulness of individual metrics [7, 44] and their visualization [45]. This underlines the statement that the "development of metrics that are valuable for assessing security and decision making is an important element of efficient counteractions to cyber threats" [21]. However, as multiple authors have pointed out, there is a lack of a link between information security metrics and management goals [4, 6, 17, 19, 38].

2.2 Information Security Management

Information security management is currently based on international standards and best practices. The ISO/IEC 27000 series is one of the most used standards and defines an information security management system (ISMS). The ISMS is based on risk assessment and the individual risk acceptance level of an organization. "It is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security to achieve business objectives" [28]. Besides the ISO/IEC 27000, there are other well-known frameworks and best practices like the NIST 800 series, COBIT, ISF, and NIST. Not all of them deal exclusively with information security management but they all do at least deal with parts of it. These documents define certain metrics for measuring the effectiveness of the ISMS. However, these metrics do not completely cover the minimum security requirements [36], and they struggle in structure and clarity as a recent study of McKinsey & Company pointed out [9].

Soomro et al. [47] introduced a literature review on information security management and concluded that a holistic view on information security is missing in the literature. Based on this argumentation, Diesch et al. [20] developed a comprehensive model of management success factors for information security decision-makers based on standards, a state-of-the-art literature analysis, and an expert interview series. The model proposes 12 management success factors that have to be taken into account when making information-security-related decisions and deriving corrective actions. These factors are access control, awareness, infrastructure, vulnerability, physical security, CIA triad, continuity, risk, compliance & policy, security management, organizational factors, and resources. The first five factors are defined as key security indicators and the root cause of information security management decisions. As suggested within this article, these management success factors serve as management goals for this research. These categories were used because no other comprehensive model or theory was present in the literature - to the best of the authors knowledge.

3 METHODOLOGY

This section describes the methodology used to define metrics within current literature (section 3.1). It also describe the Goal-Question-Metric approach to link the metrics to management success factors (section 3.2).

3.1 Literature Analysis

The literature analysis has the goal to define metrics used in practice for describing aspects of information security. To reproduce the process of getting literature sources, the method of Webster and

Table 1: Literature search process.

Data source	Hits	Reduction	Relevant
OpacPlus	132	25	15
ScienceDirect	489	12	4
Google Scholar	100	6	5
Standards		2	2
Total	**721**	**45**	**26**

Watson [54] was used. To obtain the most relevant literature in the search process, a keyword search was performed within academic databases. The searched databases were ScienceDirect, OpacPlus, and Google Scholar. OpacPlus is a wrapper that encompasses multiple databases like Scopus, Elsevier, IEEE Xplore, and Wiley to mention just a few. The search within Google Scholar was limited to the first 100 articles because the most relevant sources always appear on the first page [46]. The search string that was used to get the initial list of articles was: *"(information OR cyber) AND security AND (metrics OR indicators OR measures)"*. The search was conducted by searching within the title, abstract, and keyword fields. The next step in the search process was to filter the number of articles according to the relevant articles by topic based on the title and abstract without duplicates. Finally, the articles were analyzed by searching for metrics. Articles that do not introduce metrics to measure an aspect of information security was excluded. All the steps and the number of articles within these steps are shown in table 1. In addition to the database search, the standards ISO/IEC 27004 [29] and NIST SP 800-55 [36] were included in the literature analysis. The 45 resulting articles in the reduction step were analyzed by the first two steps of the "open-axial-selective" approach [18], which is not just the definition of clusters to a whole article but is about assigning first-order-codes to the content of the articles. The resulting metrics were first-order-codes. The second step is to combine synonyms and their meanings into second-order-codes. These are the result metrics for the step described in the following section 3.2. With this approach, metrics are included that are part of standards and best practices or are introduced by academic literature to measure aspects of information security.

3.2 The Goal-Question-Metric Approach

The Goal-Question-Metric approach [5] is the most known and accepted method to develop goal-oriented metrics. One requirement for metrics is, that they should be goal-oriented by definition. Therefore, the last step of the previously stated "open-axial-selective" approach, which would be clustering the metrics by their meanings, is replaced. A clustering from bottom to top would result in metric-oriented clusters. Instead, a top-down approach from management success factors to metrics was used to cluster the metrics defined in the previous step. First, the 12 given management success factors (section 2.2) were used as goals for management. Second, questions were developed to explain aspects of each given goal. Last, the given metrics were assigned to the questions in order to quantify aspects of the goals. Metrics that could not be assigned in order to answer a given question were considered to be not goal-oriented.

Table 2: Symbols used for information security metrics.

Symbol	Meaning	Example
%	Percent	% user accounts in compliance
Σ	Sum of	Σ admin violations
Ø	Average	Ø attack path death

4 METRICS AND THEIR LINK TO MANAGEMENT GOALS

Each management success factor [20] was given numerous questions that were derived from different standards and the problems described in the literature. The questions not only result from the literature analyzed but also from the clustering of the different metrics. The Goal-Question-Metric approach resulted in 50 questions that describe aspects of the 12 management success factors. The analysis of the 45 scientific articles of which 26 articles described different security metrics resulted in 322 metrics as first-order-codes. The linkage stage - included the elimination of duplicates - resulted in 195 metrics linked to the questions and, therefore, to the management goals.

The following subsections describe each factor with their related questions and metrics as well as how they quantify the given information security management goal. The metrics include several symbols. Table 2 show the meaning of each symbol with an example.

4.1 Access Control

The goal of **Access Control** is the regulation and minimization of access to applications, data, and infrastructure. The main challenges are off- and on-boarding processes and rules like "bring your own device" [20] which increases the difficulty to manage access control.

Table 3 shows the related questions and the consolidated metrics from literature. Three main areas are important for organizations. First, the user accounts which are present in the infrastructure have to be compliant with given rules. Second, the users with extended rights on systems have to be monitored, because the misuse or corruption of these identities can cause great harm which results in an increased risk for the organization. The last area of interest are indicators of how strong the protection is. This area includes multiple metrics that count violations related to access control which indicates weak protection as well as possibilities to test the access control protection without having a violation. For example, the average password crack time indicates whether the passwords of identities are strongly protected against these types of attacks. All percentages and averages are based on the underlying number of available constructs described within the metric. The "% password matches minimum requirements" is calculated as $\frac{\Sigma Passwords\ match\ minimum\ requirements}{\Sigma Passwords}$.

4.2 Awareness

Awareness contains all activities and countermeasures to aware employees, managers and all people about information security issues and can not be treated by technical solutions. Metrics within this area deal with awareness training, awareness violations, and

Table 3: Metrics to quantify access control.

Question	Metric
Are user accounts compliant?	% user accounts in compliance [13]
Which users have admin rights?	Σ users with admin password or superuser or root privileges [11, 36, 50]
How strong is the access protected?	Σ unauthorized access/intrusion successes [13, 16, 25, 36, 41], Σ strong credential keys [11], Σ failed logon attempts [13, 41], Σ logon violations [32], Ø password crack time [12, 27, 29], Σ attempts to change security settings [25], % password matches minimum requirements [29, 40], % optional two factor authentication [40]

business management. To give an overview of information security awareness, the information security department or management must have an overview of the current users or employees within the organization. This leads to metrics like "Σ users" that are not related to information security in the first place but have to be monitored in order to calculate percentages out of it. Also, all departments of an organization should be involved in the information security department in order to meet information security requirements. A major area of interest is the awareness training. This area is strongly represented in literature as well as measures to assess violations related to awareness policies. The most cited author within this area is Torres et al. [50] which defines multiple metrics to measure information security awareness training. The related questions are shown in Table 4.

4.3 Infrastructure

The **Infrastructure** is in contrast to vulnerabilities about the hardening of systems and all the components of the infrastructure. It is not just about hardening but also about knowledge of the infrastructure, its components, and also what attacks can occur within it. Table 5 shows the different areas of interest. The most crucial part is the questions about the knowledge of the current infrastructure of an organization. If an infrastructure component is not known or not managed by the security department, it has to be considered as not protected. The overview of the configuration state, the available communication channels as well as which components are monitored is asked to give an idea of possible attack vectors to the given infrastructure. Even if there are no official vulnerabilities reported to the current versions, accessible communication channels, and patch states there is the possibility of compromise through the given attack vector. The base to calculate percentages as well as averages is the number of systems within the infrastructure and therefore is also a metric within the question if all components are known. In practice, the term system has to be defined to set the scope of measurement and gain common acceptance.

Table 4: Metrics to quantify awareness.

Question	Metric
Are all users known?	Σ users [32], % individuals screened before enter the organization [36]
Are departments involved in information security issues?	% departments represented in the security committee [27]
Do employees violate against awareness policies?	Σ admin violations [13, 41], Σ unauthorized access to web sites/documents/files [25, 41], Σ reasons for revocation [32], Ø of user population revoked [32], Σ personnel reprimanded or fired for security decisions/actions [23]
Are employees trained and aware?	Σ best security practice incentives [50], Σ incidents reported per employee [27, 36, 50], Ø training hours received per year [50], degree of awareness (survey) [50], % security budget spent on training [50], % satisfactory accomplishment per training activity [3, 50], degree of organizational climate satisfaction [50], Ø users briefed [32], % managers with a NDA [27], Σ employees with exclusive dedication to information security [27], % managers with information security certification [27, 36], % personnel with security training (to their specific responsibilities) [3, 23, 29, 36]

4.4 Vulnerabilities

The goal to minimize **Vulnerabilities** within organizations is one of the most important goals that information security managers have. Vulnerabilities are connected to all management activities because they cause risks in case of available threats and, therefore, loss when they are disregarded. Vulnerabilities are seen in practice as technical vulnerabilities. Consequently, this management success factor is bound to be technical in nature which leads to the technical metrics shown in Table 6. To measure existing vulnerabilities the infrastructure has to be known and monitored. If systems are not monitored and updated, these have to be considered as vulnerable to attacks. Not just the monitoring itself but also the testing of infrastructure components lead to an improvement of the current information security status. A typical drawback by measuring information security vulnerabilities is the fact, that there are vulnerabilities that are not publicly available. These called zero-day exploits have to be taken into account when dealing with vulnerability metrics. It could create the wrong impression of security for managers.

Table 5: Metrics to quantify infrastructure security.

Question	Metric
Are all infrastructure components known?	Σ systems [8, 43], Σ critical assets [31, 48, 50], Σ critical areas [50], Σ applications [31, 48], % asset visibility [8, 23, 43]
Are all components configured according to the definition?	Σ configuration weaknesses [16], % secured configurations [50], Σ security evaluation deficiency [12], Σ misconfigured devices [41], Σ firewall devices with retrieved configuration [7], % system interfaces accepts only valid input [7]
Are there newer versions of components or their services available?	% available patches applied [13, 36], Σ devices requiring remediation [41], % total hosts that require remediation [41]
Are all documented components available?	% configuration available [40], % assets with control reviews [23]
Are all communication channels known?	Σ external communication paths [11], Σ remote accesses and wireless devices [36, 50], Σ access points [12]
Are all components protected against known attacks?	Σ detection mechanism deficiency [12], Σ pc/servers with antivirus installed [3, 27]
Are all components owned and monitored?	% information system assets with owners [27], % log files monitored [25, 29]

Table 6: Metrics to quantify vulnerabilities.

Question	Metric
Are all security patches up to date?	% available patches applied [13, 36], vulnerability exposure [11, 31], Σ security evaluation deficiency [12]
Are all infrastructure components known?	see infrastructure
Are all components scanned for vulnerabilities?	% tested/assessed systems [3, 8, 50], % secured areas [50], % withstand targeted pentest attacks [7]
Are all published vulnerabilities of the infrastructure known?	Σ known vulnerabilities [2, 7, 11–13, 15, 16, 29, 31, 36, 37, 41, 48], Ø vulnerabilities per system [11], % systems without severe vulnerabilities [31]

4.5 Physical Security

The physical protection of buildings, infrastructure, offices, and other hardware is a special topic in conjunction with information security. **Physical Security** is related to information security but mainly it is not part of the organization‘s information security department but of corporate security [20]. Therefore, Table 7 include just metrics related to the physical protection of infrastructure components which are critical for the business of an organization as well as the underlying number of critical systems. The number of resulting metrics also represent their presence in literature.

Table 7: Metrics to quantify physical security.

Question	Metric
Are critical components physically protected?	% critical equipment with adequate physical protection [29, 36, 50], host criticality [31, 48]

Table 8: Metrics to quantify CIA.

Question	Metric
Are all documented components available?	Ø service availability time [16, 30], % network reachability [48], % systems availability [50]
Are communication paths encrypted?	data transmission exposure [12], Σ unauthorized information disclosures [41], % encrypted communication [40], % media that passes sanitization procedures [36]

4.6 CIA Triad

The **confidentiality, integrity, and availability (CIA)** are the "protection goals" of information security but are called in practice as a theoretical construct from research. When it comes to decision-making, practice shows that management depends less on these protection goals than expected [20]. Nevertheless, the goal to protect confidentiality, integrity, and availability is very important in terms of communication and the understanding of certain countermeasures. Also, risks can be explained more easily when explaining the impact based on the CIA construct. The literature has shown the difficulty of measuring these attributes but provides metrics for consideration. These metrics are summarized in Table 8. It is also visualized in the low amount of metrics conducted out of the literature. Metrics can be used to quantify the availability of networks, documents, and systems. Aspects of confidentiality and integrity are just be measured indirectly by providing encrypted communications and perform tests which, in the case of outliers, indicate possible violations such as transmission exposure.

4.7 Continuity

Continuity is in contrast to the availability, not just the availability of systems but the continuous delivery of the intended outcome. This includes business continuity as well as systems continuity and is a major goal of information security and business management. The most questions arise in case of a malfunction or disaster in which the system must be recovered as quickly as possible. The questions and metrics present in literature and shown in Table 9 is related to the possibility and the test to recover systems and services as well as a buffer of available resources.

Table 9: Metrics to quantify continuity.

Question	Metric
Are backups for components in place?	Σ data recovery testing [50], Σ protected files [50]
Is it possible to recover a malfunction service?	Ø mean-time-to-repair systems [11, 30], Ø business critical data recovery time [50], Ø critical data recording date [50]
Do activities impact continuity?	patch risk [48], Ø systems mean-time-to-failure [30], Ø mean time to catastrophic failure [30], Σ remaining storage capacity [11–13], Σ point solutions [50]

4.8 Risk

Information security management standards are mostly based on a risk management approach. The assessment of available **Risks**, their classification and the development of countermeasures are therefore the main activities for information security managers. Minimizing risks according to the risk acceptance level is, therefore, an important goal for information security managers. The metrics and questions arising within this section are strongly related to the risk definition. Risks are present if an asset has a vulnerability and a possible threat. To quantify the risks, the impact and probability of occurrence have to be considered. Each organization has its risk acceptance and risk appetite. The metrics in Table 10 are present in the literature and quantify the different aspects described.

4.9 Compliance & Policies

Compliance & Policies come from different sources like the security management of an organization, laws, regulations, and other requirements. The goal of the management is to comply with these regulations in order to achieve certifications or not violate laws. The challenge is that a fully compliant organization may not mean a fully secure organization [20]. These written rules have to be monitored in order to evaluate their effectiveness. If no policies are in place, it is difficult to push regulations through when violating them. Therefore, the first question within Table 11 refers to the existence of policies. Policy violations and the opposite, the compliance to policies, are also measured by literature. An important topic in literature is, that policies are backed up by the management.

Table 10: Metrics to quantify risks.

Question	Metric
Are there vulnerabilities?	see vulnerabilities
Are exploitable threats available?	Ø CVSS score [48], processor or bandwidth utilization [13, 23], Σ identified potential threats [13, 15, 23, 50]
Are all components of the infrastructure related to a risk?	Ø computer/host criticality (location, application, role) [31, 48], % software and hardware classified [50], % assets with completed risk assessment [3, 22, 23, 50], % risk assessment automatization [50]
What is the probability?	% probability of compromise [13], Ø attack path death [12], Σ attack surfaces [2]
What is the impact in case of occurrence?	Σ worst case loss [11, 12, 43], Σ business value [31]
What is the current risk level?	Σ value at risk [13], Ø level of risk by area [50], risk level [16, 23, 31, 43], risk exposure [31], downstream risk [31], Σ it risk [22, 41]
What is the accepted risk level?	risk acceptance level [23], Σ risks accepted [23], Σ high risks accepted [23]

Table 11: Metrics to quantify compliance.

Question	Metric
Are policies in place?	Σ security policies/controls [43, 50], % policies and procedures into the design phase [50]
Are there policy violations?	% user accounts in compliance [13], maturity level of current controls [50],, Σ policy violations [41]
Are policies accepted by the management?	% policies and procedures documented and approved [50], % strategy robustness [50], % managers involved in the information security policy definition/evaluation/review [27]
Are all rules fulfilled?	% compliance [13, 16, 43, 50], Σ systems certified [43], Σ audits outsourced/internal [7, 23, 36, 50], % fulfilled regulations [50], % security requirements addressed in third party agreements [29]

4.10 Resources

Resources does not just mean financial budgets but also includes an appropriate number of skilled people and the appropriate time to perform the necessary tasks. Thus, the effectiveness of resource investment and employee management, as well as the availability of time for projects, is shown in Table 12. The problem when quantifying the effectiveness of security investments is, that they are not easy to understand and to use. To calculate the return on security investment (ROSI), it is necessary to assume the loss expectancy in case of corruption, the mitigation ratio for a proposed solution as well as the cost of the solution. These preconditions alone are difficult to measure and quantify. However, if this process is carried out carefully, not only the information security management but also the business will understand the value of information security.

Table 12: Metrics to quantify resources.

Question	Metric
Are projects in time?	Ø project delays [50]
Is budget enough and effectively used?	ROSI [10, 13, 50], security investment benefit [43], security budget segregation/evolution [50], Σ cost-benefit [3, 31], information security budget in current year [27], cost and effort of patch process [37], % budget devoted to IS [36]
Is there enough qualified staff?	% qualified IS staff [27, 50], % responsibility sharing [36, 50], % in house specialized staff dedicated to assessment of info-sec activities [50]

4.11 Security Management

Information **Security Management** has the goal of developing, implementing and improving information security within organizations. This goal can be achieved by implementing processes that are described in multiple standards and best practices like ISO/IEC 27000 [28], NIST 800, ITIL, and COBIT. To quantify aspects of the effectiveness of the information security management, questions have to be answered regarding the processes of the information security management program. The area of information security management processes is well described in scientific literature as well as in current standards and best practices. The sanitation of available metrics from this area shows, that the metrics are quantifying the effectiveness of typical information security processes or the ability to cover and detect attack attempts. The typical metrics contain a time component or a percentage processing of existing tasks. However, operational security does not quantify aspects of information security but the ability of an organization to detect, plan, and process information security-related tasks in an effective way. This is important for the management to continuously improve and maintain the security status of the organization. Also, Lee et al. [33] reveals, that a higher security standard does not necessarily lead to a higher security level. Table 13 shows the overview of the related questions with the metrics from the literature. There are multiple examples illustrates this. The number of viruses detected and isolated shows that viruses can be detected and the ability of the security staff to isolate them. This indicator does not cover any other aspect but the effectiveness of the security operations department. Nevertheless, if information security operations is not in place, it could be argued, that the security of an organization is not protected at all. Thus, information security operations have to be monitored and also improved in order to improve the information security status of an organization in a structured way. Another example is the average known vulnerability days which indicates how long a known vulnerability exists. The metric measure the effectiveness of vulnerability management but not the actual state of vulnerabilities within the organization. Both aspects are important but measure different things.

4.12 Organizational Factors

Organizational Factors must be considered by making information security-related decisions but can not be converted into a goal for the information security manager [20]. This factor might have an impact on whether it is possible to push policies and countermeasures through an organization or have an impact on the risk appetite as well as the possibility to hire their own staff related to information security. However, an optimal organizational size or structure is not achievable by the information security management. There are no metrics described in the literature that quantify aspects of this factor.

5 DISCUSSION AND FUTURE RESEARCH

This study synthesizes available information security metrics and links them to management success factors. To achieve this link, each management success factor was extended by questions with the help of the Goal-Question-Metric approach. Each question explains a different aspect of the related management success factor. Metrics from the literature, revealed with the help of a systematic literature review, were then assigned to one or more of the questions. Assigning these metrics leads to a clustering of available security metrics in the literature to management goals. That was asked by multiple authors in literature and requested by practitioners. This research enables security practitioners to look for specific metrics that can be used to quantify a specific goal and improve it over time. This opportunity is especially useful for small- and medium-sized businesses because they might not have the expertise to develop their own goals with specific metrics.

The distribution of metrics leads to the conjunction that there might be a set of core metrics that are required because they measure aspects of multiple goals at once. This explains the overlap of some of the metrics. An example is "known systems" which is important for understanding the infrastructure as well as it is for recognizing vulnerabilities. This turns out to be the case because an unknown and therefore not monitored system has to be defined as vulnerable. If an organization wants to establish metrics, these metrics would have the biggest impact on the organization‘s information security.

Clustering and calculation of the metrics show that some metrics are dependent on others. The best example is the risk goal. This goal can be reached by quantifying the goal of minimizing vulnerabilities as well as by knowing the infrastructure and, therefore, the threat landscape. Also, possible risks can occur from all key security indicators as shown in a previous study [20]. The assigned metrics also show these dependencies through their calculation. This means that some metrics must be implemented before others can be applied and, thus, are their prerequisites. Practitioners and researchers also have to consider the prerequisites to collect the different data that are needed to instantiate the metrics. There, the cost and effort of collecting these data have to be weighted. Also, managers with less information security background are able to look over the different aspects and easily assess the needed tasks to protect their organization. An example would be, if a metric like Σ known systems is suggested, an organization has to think about implementing a configuration management database or asset system in order to quantify this metric. Also, an infrastructure scanning

Table 13: Metrics to quantify security management.

Question	Metric
How effective are problems handled?	Ø mean-time-to-repair systems [11, 30], Σ viruses detected and isolated [13, 41, 50], % audit items closed [13, 22], time between vulnerability discovery and repair [11], Ø known vulnerability days [12], Ø time to respond to incidents [50], % incidents stopped per month [3, 50], % nonconformity aspects fixed [50], certification status (hours needed to achieve certification) [50], % audit findings closed, [22], min/max/mean time to correct a variance [23]
What external partners have to be managed?	Σ contracts with third parties [29, 50], % outsourced information security processes [50]
Which attacks and problems can be detected by the security management?	Σ incidents [22, 25, 27, 29, 36, 50], Σ packets dropped by firewall [13], Σ viruses detected in user files/e-mails/websites [13, 41], Σ intrusions detected/attempts [13, 41], Σ spam (not) detected/filtered/false-positive [41], Σ firewall false negative [7]
Are changes handled through security management?	Σ changes in compliance [12, 16, 27, 36], Σ system configuration changes[11], Σ architecture changes [50], min/max/mean time to discover a configuration variance [23]
Are countermeasures/actions planned and implemented/done?	Σ successful implementations of security procedures [43], evolution of information security plan of action [50], % daily monitored processes [50], % monthly systems performance and assurance scheduled activities [36, 50], % maintenance processes executed [50], % countermeasures implemented [50], Ø risk assessment review time [50], Σ managers monitored [27], % risk management actions planned/approved/rejected [22], Σ privacy risk monitoring activities and reports [22], Σ policy exception reviews [23], frequency of control reviews [23], maintenance delay per event [29, 36],
Is the top management involved?	% suggested procedures approved [50], % policies and procedures documented and approved [50], % strategy robustness [50], Σ downstream and upstream info-sec communication (meetings to top level management) [50], Σ managers attending the security committee meetings [27], % business initiatives supported by information security [3], % agreements with information security clauses [3]
How effective are other security related processes?	Ø hours dedicated to policies and procedures design/implementation/reviews/updated [50], % high-impact incidents on processes not contemplated in previous risk assessments [50], % internal audits accomplished [7], Ø attendees per brief [32], Ø average system approval time [32], Σ actualization's distributed in the last two weeks [27], Σ corrective actions taken after specific event [25, 29], Σ newly identified it risks [22], Σ remediations applied by time and type [41], Ø time to patch systems [37], Σ reviews by third parties [29]

tool, which reveals hidden systems is needed to distinguish between known and unknown systems. This result in the need for thinking about the availability of data, their usefulness, and accuracy.

Multiple authors have mentioned the same metrics but have articulated them in different wording, scales or contexts. There were also authors that mentioned multiple metrics in the same article, but they had the same meaning although they had different names. This makes it clear that there is still no common understanding of information security metrics in the literature. This study can help to determine such an understanding.

Previous work deals with multiple suggestions about specific metrics. These metrics are helpful to measure certain aspects of information security. This work combines the information security management perspective with the technical information security metrics view to link them together so that a practitioner and a researcher have the ability to understand each other‘s needs and background. The research of information security metrics was extended by clustering them to management success factors as well as the other way around.

Each study has its limitations and creates opportunities for further research. The literature survey was rigorously conducted using the proposed methodology but is limited to the asked databases and, thus, might not contain each relevant article. Also, the filtering process as well as the analysis and assignment steps were done to the best of the authors‘ knowledge but could include subjective meanings of the authors. An empirical study can be conducted to evaluate the proposed metric assignment as well as the usability and understandability of the metrics. The information security management has the opportunity to choose or implement all the proposed metrics, but the number of them is very large which could lead to information overload effects. Therefore, future research could investigate combining and aggregating the different metrics from the individual goals to develop a key indicator for each goal that could then be presented to the information security management. Such an information security management dashboard was asked by different experts in the field [20] and is requested in recent research articles [1, 34, 49]. The proposed systematization of metrics from the literature can serve as the basis for such dashboard developments as well as research in the field of quantifying and developing key security indicators. A further research possibility could be the design, architecture, and development of a solution to automatically collect the necessary data for security metrics from an organization. Also, a question remains if all metrics are really necessary and useful to measure the actual information security status of an organization. An example would be spending hours on training and if the awareness increases with more training hours. Especially if the training itself is not effective. Other authors criticize metrics within standards and best practices regarding their objectives. They measure the effective implementation of countermeasures and not the actual information security status of an organization or if the countermeasures itself are effective [7]. This applies mainly to metrics within the "security management" cluster within this article. The detailed discussion of each metric depends on the context and is out of scope of this research article. It can be argued that these metrics are not useful for measuring the actual information security status but the effective implementation of processes and countermeasures. Therefore, future research should empirically test the proposed metrics in order to evaluate their meaningfulness and usability in measuring the actual information security status of an organization.

6 CONCLUSION

Information security metrics are the most common method to measure the effectiveness of information security countermeasures and concerns in organizations. There are many metrics described in the literature. However, they are not related to security management goals. Therefore, this study investigates how information security metrics from the literature can be linked to security management goals.

To answer the research question, a state-of-the-art literature analysis was conducted to define metrics. After that, 12 management success factors were defined as management goals. The Goal-Question-Metric approach was used to specify different aspects of the goals. Finally, the metrics were assigned to the developed questions in order to cluster the metrics to the information security management goals.

The results combined the two research streams of information security metrics and information security management objectives. Therefore, it helps to understand what the metrics quantify from the management perspective and the other way around. The results can be used to further develop key indicators, conduct empirical studies, and investigate in the research of possible dashboards for the information security management. Also, the research can provide an opportunity to design a technical information security assessment solution.

REFERENCES

[1] Ahmed I. Al-Darwish and Pilsung Choe. 2019. A Framework of Information Security Integrated with Human Factors. In *HCI for Cybersecurity, Privacy and Trust*, Abbas Moallem (Ed.). Lecture Notes in Computer Science, Vol. 11594. Springer International Publishing, Cham, 217–229. https://doi.org/10.1007/978-3-030-22351-9{_}15

[2] Jaafar Almasizadeh and Mohammad Abdollahi Azgomi. 2013. A stochastic model of attack process for the evaluation of security metrics. *Computer Networks* 57, 10 (2013), 2159–2180. https://doi.org/10.1016/j.comnet.2013.03.011

[3] Jason Andress and Mark Leary. 2017. *Building a Practical Information Security Program*. Elsevier.

[4] M. P. Azuwa, Shahrin Sahib, and Solahuddin Shamsuddin. 2017. Technical Security Metrics Model in Compliance with ISO/IEC 27001 Standard. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)* 1, 4 (2017), 280–288.

[5] V. R. Basili and D. M. Weiss. 1984. A Methodology for Collecting Valid Software Engineering Data. *IEEE Transactions on Software Engineering* SE-10, 6 (Nov 1984), 728–738. https://doi.org/10.1109/TSE.1984.5010301

[6] Jennifer Bayuk and Ali Mostashari. 2013. Measuring systems security. *Systems Engineering* 16, 1 (2013), 1–14. https://doi.org/10.1002/sys.21211

[7] Jennifer L. Bayuk. 2013. Security as a theoretical attribute construct. *Computers & Security* 37 (2013), 155–175. https://doi.org/10.1016/j.cose.2013.03.006

[8] Paul E. Black, Karen Scarfone, and Murugiah Souppaya. 2008. Cyber Security Metrics and Measures. In *Wiley Handbook of Science and Technology for Homeland Security*, John G. Voeller (Ed.). John Wiley & Sons, Inc, Hoboken, NJ, USA. https://doi.org/10.1002/9780470087923.hhs440

[9] Jim Boehm, Peter Merrath, Thomas Poppensieker, Rolf Riemenschnitter, and Tobias Stähle. 2017. Cyber risk measurement and the holistic cybersecurity approach. https://www.mckinsey.com/business-functions/risk/our-insights/cyber-risk-measurement-and-the-holistic-cybersecurity-approach last checked: 30.09.2019.

[10] Rainer Böhme. 2010. Security metrics and security investment models. In *Advances in Information and Computer Security*. Springer Berlin Heidelberg, Berlin, Heidelberg, 10–24.

[11] Wayne Boyer and Miles McQueen. 2007. Ideal Based Cyber Security Technical Metrics for Control Systems. In *Critical information infrastructures security*. 246–260. https://doi.org/10.1007/978-3-540-89173-4{_}21

[12] Wayne F. Boyer and Miles A. McQueen. 2008. *Primer Control System Cyber Security Framework and Technical Metrics*. Technical Report INL/EXT-08-14324. Idaho National Laboratory.

[13] W. Krag Brotby. 2009. *Information security management metrics: A definitive guide to effective security monitoring and measurement*. CRC Press, Boca Raton.

[14] Sangmi Chai, Minkyun Kim, and H. Raghav Rao. 2011. Firms' information security investment decisions: Stock market evidence of investors' behavior. *Decision Support Systems* 50, 4 (2011), 651–661. https://doi.org/10.1016/j.dss.2010.08.017

[15] Agniswar Chakraborty, Anirban Sengupta, and Chandan Mazumdar. 2012. A formal approach to information security metrics. In *2012 Third International Conference on Emerging Applications of Information Technology*. IEEE, 439–442. https://doi.org/10.1109/EAIT.2012.6408003

[16] K. Clark, J. Dawkins, and J. Hate. 2005. Security risk metrics: fusing enterprise objectives and vulnerabilities. In *Proceedings from the Sixth Annual IEEE Systems, Man and Cybernetics (SMC) Information Assurance Workshop, 2005*. IEEE, 388–393. https://doi.org/10.1109/IAW.2005.1495978

[17] Zachary A. Collier, Mahesh Panwar, Alexander A. Ganin, Alex Kott, and Igor Linkov. 2016. Security Metrics in Industrial Control Systems. In *Cybersecurity of SCADA and other industrial control systems*, Edward J. M. Colbert and Alexander Kott (Eds.). Springer, Switzerland, 167–185. https://doi.org/10.1007/978-3-319-32125-7_9

[18] Juliet Corbin and Anselm Strauss. 1990. Grounded theory research: Procedures, canons and evaluative criteria. *Qualitative Sociology* 13, 1 (1990), pp. 3–21.

[19] Rainer Diesch, Matthias Pfaff, and Helmut Krcmar. 2018. Prerequisite to Measure Information Security: A State of the Art Literature Review. In *4th International Conference on Information Systems Security and Privacy (ICISSP)*. 207–215. https://doi.org/10.5220/0006545602070215

[20] Rainer Diesch, Matthias Pfaff, and Helmut Krcmar. 2020. A Comprehensive Model of Information Security Factors for Decision-Makers. *Computers & Security* (2020). https://doi.org/10.1016/j.cose.2020.101747

[21] Elena Doynikova, Andrey Fedorchenko, and Igor Kotenko. 2019. Ontology of Metrics for Cyber Security Assessment. In *Proceedings of the 14th International Conference on Availability, Reliability and Security - ARES '19*, Unknown (Ed.). ACM Press, New York, New York, USA, 1–8. https://doi.org/10.1145/3339252.3341496

[22] Cezar Drugescu and Rafael Etges. 2006. Maximizing the Return on Investment on Information Security Programs: Program Governance and Metrics. *Information Systems Security* 15, 6 (2006), 30–40. https://doi.org/10.1080/10658980601051482

[23] Jack Freund. 2015. *Measuring and managing information risk: A FAIR approach*. Butterworth-Heinemann, Amsterdam.

[24] Daniel Geer, Kevin Soo Hoo, and A. Jaquith. 2003. Information security: Why the future belongs to the quants. *IEEE Security & Privacy Magazine* 1, 4 (2003), 24–32. https://doi.org/10.1109/MSECP.2003.1219053

[25] Kemal Hajdarevic and Pat Allen. 2013. A New Method for the Identification of Proactive Information Security Management System Metrics. In *36th International Convention on Information & Communication Technology, Electronics & Microelectronics*. 1121–1126.

[26] Karin Hedström, Ella Kolkowska, Fredrik Karlsson, and J. P. Allen. 2011. Value conflicts for information security management. *The Journal of Strategic Information Systems* 20, 4 (2011), 373–384. https://doi.org/10.1016/j.jsis.2011.06.001

[27] S.O.S. Herrera. 2005. Information security management metrics development. In *39th Annual 2005 International Carnahan Conference on Security Technology*. 51–56. https://doi.org/10.1109/CCST.2005.1594818

[28] ISO/IEC. 2018. *ISO/IEC 27000:2018(E): Information technology - Security techniques - Information security management systems - Overview and vocabulary*. Standard. ISO/IEC, Switzerland.

[29] ISO/IEC. 2018. *ISO/IEC 27004:2009(E) - Information technology - Security techniques - Information security management - Measurement.* Standard. ISO/IEC, Switzerland.

[30] E. Jonsson and L. Pirzadeh. 2011. A Framework for Security Metrics Based on Operational System Attributes. In *2011 Third International Workshop on Security Measurements and Metrics*. IEEE, 58–65. https://doi.org/10.1109/Metrisec.2011.19

[31] Igor Kotenko and Elena Doynikova. 2013. Security metrics for risk assessment of distributed information systems. In *2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS)*. IEEE, 646–650. https://doi.org/10.1109/IDAACS.2013.6663004

[32] Gerald Kovacich. 1997. Information systems security metrics management. *Computers & Security* 16, 7 (1997), 610–618. https://doi.org/10.1016/S0167-4048(97)80798-5

[33] Chul Ho Lee, Xianjun Geng, and Srinivasan Raghunathan. 2016. Mandatory Standards and Organizational Information Security. *Information Systems Research* 27, 1 (2016), 70–86. https://doi.org/10.1287/isre.2015.0607

[34] Janosch Maier, Arne Padmos, Mortaza S. Bargh, and Wolfgang Wörndl. 2017. Influence of Mental Models on the Design of Cyber Security Dashboards. In *Proceedings of the 12th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications*. SCITEPRESS - Science and Technology Publications, 128–139. https://doi.org/10.5220/0006170901280139

[35] Katarzyna Mazur, Bogdan Ksiezopolski, and Zbigniew Kotulski. 2015. The Robust Measurement Method for Security Metrics Generation. *Comput. J.* 58, 10 (2015), 2280–2296. https://doi.org/10.1093/comjnl/bxu100

[36] National Institute of Standards and Technology. 2008. *NIST SP 800-55r1: Performance Measurement Guide for Information Security.* Technical Report. National Institute of Standards and Technology.

[37] Elizabeth A. Nichols and Andrew Sudbury. 2006. Implementing Security Metrics Initiatives. *EDPACS* 34, 3 (2006), 10–20. https://doi.org/10.1201/1079.07366981/46248.34.3.20060901/94537.2

[38] Marcus Pendleton, Richard Garcia-Lebron, Jin-Hee Cho, and Shouhuai Xu. 2017. A Survey on Systems Security Metrics. *Comput. Surveys* 49, 4 (2017), 1–35. https://doi.org/10.1145/3005714

[39] Tito Waluyo Purboyo, Budi Rahardjo, and Kuspriyanto. 2011. Security metrics: A brief survey. In *2011 2nd International Conference on Instrumentation, Communications, Information Technology and Biomedical Engineering*. 79–82. https://doi.org/10.1109/ICICI-BME.2011.6108598

[40] Jaziar Radianti and Terje Gjøsæter. 2017. Metrics for Ensuring Security and Privacy of Information Sharing Platforms for Improved City Resilience. *International Journal of Information Systems for Crisis Response and Management* 9, 3 (2017), 36–54. https://doi.org/10.4018/IJISCRAM.2017070103

[41] J. Patrick Ravenel. 2006. Effective Operational Security Metrics. *Information Systems Security* 15, 3 (2006), 10–17. https://doi.org/10.1201/1086.1065898X/46183.15.3.20060701/94183.3

[42] Manuel Rudolph and Reinhard Schwarz. 20.08.2012 - 24.08.2012. A Critical Survey of Security Indicator Approaches. In *2012 Seventh International Conference on Availability, Reliability and Security*. IEEE, 291–300. https://doi.org/10.1109/ARES.2012.10

[43] Julie J.C.H. Ryan and Daniel J. Ryan. 2008. Performance Metrics for Information Security Risk Management. *IEEE Security & Privacy* 6, 5 (2008), 38–44. https://doi.org/10.1109/MSP.2008.125

[44] Reijo M. Savola. 2013. Quality of security metrics and measurements. *Computers & Security* 37 (2013), 78–90. https://doi.org/10.1016/j.cose.2013.05.002

[45] Reijo M. Savola and Petri Heinonen. 2011. A visualization and modeling tool for security metrics and measurements management. In *2011 Information Security for South Africa*. 1–8. https://doi.org/10.1109/ISSA.2011.6027518

[46] Mario Silic and Andrea Back. 2014. Information security: Critical review and future directions for research. *Information Management & Computer Security* 22, 3 (2014), 279–308. https://doi.org/10.1108/IMCS-05-2013-0041

[47] Zahoor Ahmed Soomro, Mahmood Hussain Shah, and Javed Ahmed. 2016. Information security management needs more holistic approach: A literature review. *International Journal of Information Management* 36, 2 (2016), 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

[48] Kun Sun, Sushil Jajodia, Jason Li, Yi Cheng, Wei Tang, and Anoop Singhal. 2011. Automatic security analysis using security metrics. In *2011 - MILCOM 2011 Military Communications Conference*. IEEE, 1207–1212. https://doi.org/10.1109/MILCOM.2011.6127465

[49] Harold Nguegang Tewamba, Jean Robert Kala Kamdjoug, Georges Bell Bitjoka, Samuel Fosso Wamba, and Nicolas Nkondock Mi Bahanag. 2019. Effects of Information Security Management Systems on Firm Performance. *American Journal of Operations Management and Information Systems* 4, 3 (2019), 99–108. https://doi.org/10.11648/j.ajomis.20190403.15

[50] Jose M. Torres, Jose M. Sarriegi, Javier Santos, and Nicolás Serrano. 2006. Managing Information Systems Security: Critical Success Factors and Indicators to Measure Effectiveness. *Information Security. ISC 2006. Lecture Notes in Computer Science* 4176 (2006), 530–545. https://doi.org/10.1007/11836810{_}38

[51] Zhiling Tu and Yufei Yuan. 2014. Critical Success Factors Analysis on Effective Information Security Management: A Literature Review. In *20th Americas Conference on Information Systems*. 1874–1886.

[52] R. B. Vaughn, R. Henning, and A. Siraj. 2003. Information Assurance Measures and Metrics - State of Practice and Proposed Taxonomy. In *Proceedings of the 36th Annual Hawaii International Conference on System Sciences*. https://doi.org/10.1109/HICSS.2003.1174904

[53] Vilhelm Verendel. 2009. Quantified security is a weak hypothesis: A critical survey of results and assumptions. In *Proceedings of the 2009 workshop on New security paradigms workshop*. 37–50. https://doi.org/10.1145/1719030.1719036

[54] Jane Webster and Richard T. Watson. 2002. Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly* 26, 2 (2002), xiii–xxiii.

[55] Derek Young, Juan Lopez, Mason Rice, Benjamin Ramsey, and Robert McTasney. 2016. A framework for incorporating insurance in critical infrastructure cyber risk strategies. *International Journal of Critical Infrastructure Protection* 14 (2016), 43–57. https://doi.org/10.1016/j.ijcip.2016.04.001

[56] Janusz Zalewski, Steven Drager, William McKeever, and Andrew J. Kornecki. 2014. Measuring Security: A Challenge for the Generation. In *2014 Federated Conference on Computer Science and Information Systems (Annals of Computer Science and Information Systems)*. 131–140. https://doi.org/10.15439/2014F490