Technische Universität München
TUM School of Management

Firm Compliance and Governance of Open Source Software Activities

Juliane Birgit Wissel

Vollständiger Abdruck der von der TUM School of Management der Technischen Universität München zur Erlangung des akademischen Grades einer

Doktorin der Wirtschafts- und Sozialwissenschaften (Dr. rer. pol.)

genehmigten Dissertation.

Vorsitz: Prof. Dr. Hanna Hottenrott
Prüfer der Dissertation: 1. Prof. Dr. Michael Zaggl
2. Prof. Dr. Helmut Krcmar

Die Dissertation wurde am 07.09.2023 bei der Technischen Universität München eingereicht und durch die TUM School of Management am 15.02.2024 angenommen.

Acknowledgements

The years I devoted to this dissertation feel like an unforgettable adventure marked by immense personal and academic growth, memorable personal encounters, and chasing (significance level) stars. I would like to express my heartfelt gratitude to all those who have supported me throughout this journey. Their guidance, encouragement, and unwavering belief in my abilities have been invaluable.

First and foremost, I extend my deepest appreciation to my supervisor Michael Zaggl for his continuous guidance, insightful feedback, and patience. His expertise and willingness to share his knowledge have helped me in shaping the direction of this research. I am also indebted to the further members of my dissertation committee, Hanna Hottenrott and Helmut Krcmar. Further, I want to highlight the support from Aron Lindberg and Jörn Block whose critical insights and constructive suggestions have immensely shaped this work. I extend my gratitude to the participants of my studies, without whom this research would not have been possible. Their willingness to share their experiences and insights has enriched this dissertation significantly.

I cannot stress enough how thankful I am to Joachim Henkel. Although not being my supervisor, he always offered valuable advice and encouraged me to think out of the box. It has always been a pleasure being part of his team and I am looking forward to another year in the TIM crew. Speaking of the TIM crew, I am incredibly thankful to all my colleagues who engaged in thought-provoking discussions, offered fresh perspectives, and stimulated ideas that contributed to the refinement of my research. I owe to them most of the memories I will keep from my dissertation journey.

Of course, I need to mention my friends and family whose endless support and encouragement have been a constant source of energy and motivation throughout this journey. Especially, I want to thank Michael Pütz who always told me: “If you don’t feel motivated to work on your dissertation, then do it without motivation!” All jokes aside, I could not have wished for a more inspiring mentor. Further, I am gifted with both the best godmother and grandmother on earth. Spending time with them is the greatest energy boost and usually ends with us laughing tears.

Lastly, but most importantly, I dedicate this dissertation to my parents who are the most important people in my life. No matter which path I choose, I can always count on their unconditional love. Their words of encouragement and understanding provided the emotional support that kept me motivated throughout this challenging yet rewarding journey.

Abstract

Open source software (OSS) is gaining relevance for companies of all sizes and industries. They do not only passively use OSS, but also act as contributors to OSS communities. Active collaboration with OSS communities comes along with certain challenges for companies resulting from diverging interests and ideologies. Thus, companies need to set appropriate policies and incentives that manage their employees' interaction with OSS communities. Yet, when introducing internal governance processes, companies face a significant trade-off. They need to ensure a compliant behavior towards the OSS communities, while enabling their organizational units to manage the specific contributions to OSS communities with a certain degree of flexibility.

The first study in this dissertation picks up this issue and analyzes how companies design mechanisms to govern contributions to OSS communities, while taking this trade-off into account. Results of the multiple case study at Siemens AG show that the extent of adoption of the centralized OSS contribution process and the resulting degree of flexibility depends on the level of closeness to core intellectual property of the organizational unit and the intensity of involvement in OSS communities. Further, more experienced developers have several options to shorten the process.

Governance, especially the compliance with OSS license terms, is also crucial when companies use OSS internally or implement it into own products and services. The ISO 5230 standard for OSS compliance and the related self- and third-party certification approaches should help companies in credibly demonstrating their OSS compliance to their customers and other stakeholders. The three remaining studies are dedicated to the recent phenomenon of OSS compliance certification.

The multiple case study in chapter 3 identifies several drivers, motives, and deterrents regarding OSS compliance certification from the perspective of self-certified and third-party certified companies and third-party certification bodies. The discrete choice-based conjoint experiment in chapter 4 reveals OSS compliance certification as decision-relevant criterion for selecting a software supplier. Third-party certified suppliers are chosen about 2.5 times more likely than self-certified suppliers. Awareness of the ISO 5230 standard and the perceived risk of OSS procurement are critical moderating factors. The cluster analysis in chapter 5 uncovers four distinct decision maker groups: Experience and OSS compliance certification-focused, experience and collaboration-focused, experience-focused, and OSS compliance certification-focused decision makers. In addition, it identifies several factors that can predict cluster affiliation.

Zusammenfassung

Open Source Software (OSS) gewinnt für Unternehmen aller Größen und Branchen zunehmend an Bedeutung. Sie nutzen OSS nicht nur, sondern leisten auch einen aktiven Beitrag zu Communities. Die Zusammenarbeit mit OSS Communities ist für Unternehmen mit gewissen Herausforderungen verbunden, die sich aus divergierenden Interessen und Ideologien ergeben. Daher müssen Unternehmen geeignete Maßnahmen und Anreize definieren, um das Engagement ihrer Mitarbeiter in OSS Communities zu steuern. Bei der Einführung interner Governance-Prozesse sind die Unternehmen jedoch einem Zielkonflikt ausgesetzt. Sie müssen ein konformes Verhalten gegenüber OSS Communities sicherstellen und gleichzeitig ihre Abteilungen in die Lage versetzen, ihre Beiträge zu den Communities mit einem gewissen Maß an Flexibilität steuern zu können.

Die erste Studie dieser Dissertation greift dieses Thema auf. Sie analysiert, wie Unternehmen Mechanismen zur Steuerung von Beiträgen zu OSS Communities gestalten und dabei diesen Zielkonflikt berücksichtigen. Die Ergebnisse der Multiple Case Study in der Siemens AG zeigen, dass es von der Nähe zu zentraler IP und der Intensität der Zusammenarbeit mit OSS Communities abhängt, inwiefern Abteilungen den Siemens-weiten OSS Contribution-Prozess übernehmen und anpassen. Erfahrenere Entwickler haben zudem mehrere Möglichkeiten, den Prozess abzukürzen.

Governance, insbesondere die Einhaltung von OSS-Lizenzbedingungen, ist auch dann von entscheidender Bedeutung, wenn Unternehmen OSS intern nutzen oder in eigene Produkte und Dienste implementieren. Die ISO-Norm 5230 für OSS Compliance und die damit verbundene Selbst- und Fremdzertifizierung sollen Unternehmen dabei helfen, ihren Kunden und anderen Stakeholdern die Einhaltung von OSS-Lizenzbestimmungen glaubhaft zu demonstrieren. Die drei verbleibenden Studien widmen sich diesem neuen Phänomen der OSS-Compliance-Zertifizierung.

Die Multiple Case Study in Kapitel 3 identifiziert verschiedene Treiber, Motive und Hindernisse in Bezug auf die OSS-Compliance-Zertifizierung aus der Perspektive von selbst- und fremdzertifizierten Unternehmen sowie von Zertifizierern. Das diskrete Entscheidungsexperiment in Kapitel 4 identifiziert die OSS-Compliance-Zertifizierung als entscheidungsrelevantes Kriterium für die Auswahl von Softwareanbietern. Softwareanbieter mit Fremdzertifizierung werden etwa 2,5-mal häufiger gewählt als selbstzertifizierte Anbieter. Die Bekanntheit der ISO-Norm 5230 und das empfundene Risiko der OSS-Beschaffung sind entscheidende Moderationsfaktoren. Die Clusteranalyse in Kapitel 5 differenziert vier Gruppen von Entscheidungsträgern:

Entscheider mit Fokus auf Erfahrung und OSS-Compliance-Zertifizierung, Entscheider mit Fokus auf Erfahrung und vorherige Zusammenarbeit, Entscheider mit Fokus auf Erfahrung und Entscheider mit Fokus auf OSS-Compliance-Zertifizierung. Darüber hinaus werden mehrere Faktoren identifiziert, die die Cluster-Zugehörigkeit vorhersagen können.

Table of contents

List of figures

List of tables

List of abbreviations

AG	Aktiengesellschaft (German for “incorporated company“)
AktG	Aktiengesetz (German for “Stock Corporation Act”)
ANOVA	Analysis of variance
B2B	Business-to-Business
B2C	Business-to-Consumer
CLA	Contributor license agreement
DAkkS	Deutsche Akkreditierungsstelle (national accreditation body of Germany)
DCO	Developer certificate of origin
FOSS	Free and open source software
GmbH	Gesellschaft mit beschränkter Haftung (German for “limited company“)
HSD	Honest Significant Difference
IEC	International Electrotechnical Commission
IP	Intellectual property
ISO	International Organization for Standardization
IT	Information technology
OSS	Open source software
SBOM	Software bill of materials
URL	Uniform resource locator
US	United States

1 Introduction

1.1 Motivation

Over the last years, open source software (OSS) has evolved into an intensely studied phenomenon of open innovation with substantial relevance for theory and practice (Chesbrough, 2003; Dahlander & Magnusson, 2008; West & Gallagher, 2006). OSS is rooted in the principles of crowd-based knowledge creation and decentralized collaboration (Blohm et al., 2011; Leimeister et al., 2009; Zaggl et al., 2023) and thus represents a paradigm shift regarding how organizations can leverage and exploit innovation (Feller et al., 2008; Forte & Lampe, 2013). At its core, OSS involves the voluntary contribution of source code, associated documentation, and other resources from individuals or organizations to public repositories that are freely accessible and modifiable by a global developer and user community. This collaborative environment facilitates a collective problem-solving approach and fosters the exchange of diverse perspectives and skill sets. The openness of the source code encourages continuous validation and improvement through the community (S. Daniel, Midha, et al., 2018; Howison & Crowston, 2014; J. Lee et al., 2022).

Apart from these opportunities that stem from the unique nature of OSS communities as decentralized and voluntary ecosystems, it also comes along with certain challenges. One challenge is related to community governance and decision-making. The absence of a centralized control body can impede coordination, conflict resolution, and the definition of the project vision. Hence, the establishment of certain governance structures and decision-making mechanisms in OSS communities is crucial (Lindberg et al., 2016; O'Mahony, 2007; O'Mahony & Ferraro, 2007). Further, the success of OSS projects largely depends on constant community engagement. Motivating steady contributions from volunteers and attracting new developers are essential for community vitality (S. Daniel, Midha, et al., 2018; Ke & Zhang, 2010; Krogh et al., 2012; Krogh et al., 2003; Shah, 2006; Spaeth et al., 2015).

Companies across all industries have realized the potential of OSS. They do not only passively use OSS, but also act as active contributors. If companies manage to leverage the potential of OSS, it can help to accelerate software development, reduce time-to-market for new products and services, and improve cost effectiveness (Chengalur-Smith et al., 2010; West & Gallagher, 2006). Active participation in OSS communities can increase a company’s reputation by showing commitment to knowledge sharing and collaboration. In addition, companies can spread their standards and influence the project direction to a certain extent (Ågerfalk & Fitzgerald, 2008; Macredie & Mijinyawa, 2011; Rolandsson et al., 2011).

Yet, the engagement of companies in OSS communities also leads to certain challenges. Communities need to ensure that all participating parties comply with their requirements and contribute to the community objectives, whereas companies have to minimize the risk of inappropriate knowledge spillovers, protect company reputation, which may be hurt by low-quality contributions, and avoid violation of intellectual property (IP) rights. Thus, both parties demonstrate diverging interests and ideologies that somehow need to be balanced to enable collaboration (O'Mahony & Bechky, 2008). The interaction requires governance of community as well as company activities (Dahlander & Magnusson, 2008). Companies, for example, need to set appropriate policies and incentives that manage their employees' interaction with OSS communities (S. Daniel, Maruping, et al., 2018; Mehra et al., 2011).

Governance is not only required when companies interact actively with OSS communities, but also when they use OSS internally or implement it into own products and services. When doing so, companies need to ensure that they comply with OSS principles (Morgan et al., 2013). OSS compliance refers to OSS users, integrators, and developers respecting copyright notices and abiding by obligations that come along with the different OSS licenses (Haddad, 2016). Companies insufficiently managing their OSS compliance risk violating license terms, which can result in litigations, leading to significant financial and reputational losses for companies (Harutyunyan, 2020). A prominent example is the lawsuit CoKinetic Systems filed against Panasonic Avionics in 2017, seeking damages of over $100 million. CoKinetic Systems, an in-flight entertainment software manufacturer, claimed that Panasonic Avionics breached the GPL license terms by intentionally refusing to reveal the source code for its open source Linux-based operating system[1]. Although the case ultimately has been dismissed, it caused undesirable publicity for Panasonic Avionics. Another example is the lawsuit that was initiated by the Free Software Foundation against Cisco Systems in 2008, involving several cases of GPL license terms violation. In 2009, a settlement could be reached. Cisco had to appoint a director with the responsibility to ensure compliance with OSS licenses for Linksys products. Further, Cisco made an undisclosed financial contribution to the Free Software Foundation[2].

[1] https://www.mend.io/blog/the-100-million-case-for-open-source-license-compliance/, retrieved August 8, 2023

[2] https://www.fsf.org/news/2009-05-cisco-settlement.html, retrieved August 8, 2023

To avoid such conflicts, companies increasingly realize the importance of the topic OSS compliance. Yet, managing compliance is complex, especially when companies acquire software that contains OSS components from external software suppliers. In 2016, a new standard has been developed by the OpenChain Project[3] to facilitate OSS compliance. Since 2020, this standard is also an official ISO standard (ISO/IEC 5230). It defines the core measures for OSS compliance and makes it possible to ensure compliance. Based on this standard, companies can achieve a self-certification or third-party certification (The Linux Foundation, 2022). For self-certification, companies can fill in an online questionnaire and upload documentation as evidence for fulfilling the essential criteria for being OSS compliant. Alternatively, companies also have the option to be certified by different third-party certification bodies. In the software supply chain, this certification is supposed to help software suppliers in credibly demonstrating their OSS compliance to their customers and other stakeholders.

The growing importance of OSS compliance for companies and the newly evolving phenomenon of a corresponding certification provide numerous research opportunities and set the playing field for this dissertation. Research is needed to understand how companies govern their contributions to OSS communities. Moreover, the question arises what motivates companies to achieve OSS compliance certification. Finally, it is worth investigating which role such a certification plays in the software supplier selection process. In the following chapter, the research objectives and designs are outlined in more detail.

1.2 Research objectives

The core themes of this dissertation are OSS contribution governance and OSS compliance. OSS contribution governance thereby refers to the processes companies implement to govern their employees' engagement in OSS communities. In contrast, OSS compliance refers to OSS users, integrators, and developers respecting copyright notices and abiding by obligations that come along with the different OSS licenses (Haddad, 2016).

The research projects described in the four chapters of this dissertation can be sorted into Dahlander and Gann's (2010) taxonomy of open innovation processes, which consists of two dimensions (see Figure 1-1). The first dimension is divided into inbound and outbound innovation. Inbound innovation refers to "how firms source and acquire expertise", outbound innovation to how companies bring "their ideas and resources to the

[3] https://www.openchainproject.org/, retrieved August 8, 2023

marketplace" (Dahlander & Gann, 2010, p. 700). The second dimension describes whether pecuniary or non-pecuniary interactions are involved. This leads to the four open innovation process categories of revealing, selling, sourcing, and acquiring. According to the authors, revealing is defined as "reveal[ing] internal resources without immediate financial rewards, seeking indirect benefits to the focal firm" (Dahlander & Gann, 2010, p. 703). Selling refers to "how firms commercialize their inventions and technologies through selling or licensing out resources developed in other organizations" (Dahlander & Gann, 2010, p. 704). Sourcing describes "how firms can use external sources of innovation" (Dahlander & Gann, 2010, p. 704). Acquiring is defined as "acquiring input to the innovation process through the marketplace" (Dahlander & Gann, 2010, p. 705).

As described in chapter 1, a successful collaboration between OSS communities and firms requires governance of community as well as company activities. Prior literature addresses this phenomenon mainly by focusing exclusively on OSS governance from the community perspective (O'Mahony & Ferraro, 2007). From the company perspective, researches have acknowledged the need for formalized instruments and processes on the company side to mitigate the risks associated with collaboration across companies and OSS communities (Germonprez et al., 2012). Yet, when introducing certain internal governance processes, companies face a significant trade-off. They need to ensure a compliant behavior towards the OSS communities, while enabling their organizational units to manage the specific contributions to OSS communities with a certain degree of flexibility. We lack insights into how companies design mechanisms to govern contributions to OSS communities, while taking this trade-off into account. This leads to the following research objective:

Research objective 1: Develop an understanding of how companies manage the trade-off between controlling their employees and granting them a certain degree of flexibility in their community engagement when designing certain OSS contribution governance mechanisms.

This research objective is covered in chapter 2. It is related to the open innovation process type "revealing" in Dahlander and Gann's taxonomy (see Figure 1-1). It deals with contributions from companies to OSS communities and thus looks at outbound, non-pecuniary interactions. Addressing this research objective is valuable, as it provides further insights into how companies manage the interaction with OSS communities and how they do justice to the fact that their different organizational units have specific needs regarding their OSS community engagement. The insights enhance the literature on company-involved OSS development (Ågerfalk & Fitzgerald, 2008; S. Y. Ho & Rai, 2017; Macredie & Mijinyawa, 2011; Rolandsson et al., 2011). More concretely, they contribute to the literature on OSS contribution governance (Germonprez et al., 2017; Germonprez et al., 2012; O'Mahony & Ferraro, 2007). Further, addressing this research objective can provide valuable recommendations for practitioners on how to accommodate organizational unit-specific requirements when designing OSS contribution governance processes to allow for the greatest possible profit from the OSS community involvement.

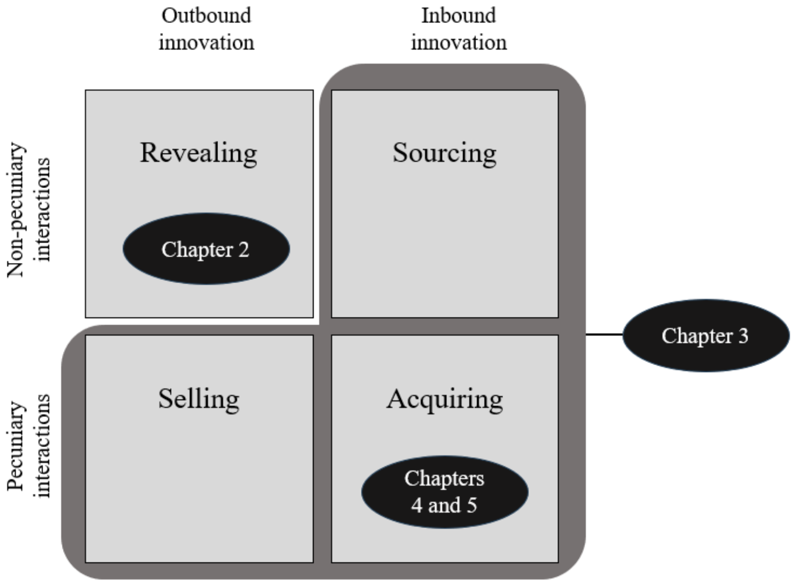


Figure 1-1: Chapters sorted into Dahlander and Gann's (2010) taxonomy of open innovation processes

The recent phenomenon of OSS compliance certification opens several research opportunities. While in the past the OSS ecosystem strongly based on trust and personal connections inside the community, the question arises why companies see the need for an ISO standard regarding OSS compliance and a related certification. In addition, the rather unique characteristic of this certification to offer not only a third-party but also a self-certification approach is a factor worth being investigated. The two differing certification approaches point at potentially differing motives and deterrents.

While literature has already examined motives and deterrents regarding several established ISO standards (e.g., ISO 9000) (Anderson et al., 1999; Quirós & Justino, 2013), ISO 5230 is a relatively new standard. Hence, the second research objective arises:

Research objective 2: Identify drivers for OSS compliance certification and develop an understanding of what motivates or prevents companies from attaining self- or third-party certification.

Chapter 3 deals with this research objective. When looking at Dahlander and Gann’s taxonomy, the objective relates to three of the open innovation processes:

Sourcing, acquiring, and selling (see Figure 1-1). The study in chapter 3 considers the motives for and deterrents to OSS compliance certification from the perspectives of companies that use OSS internally (sourcing), that integrate OSS into own products and services (selling), and that purchase software or hardware that contains OSS components from suppliers (acquiring).

Insights from this study are valuable for theory and practice. It contributes to the literature on ISO certification (Anderson et al., 1999; T. Y. Lee, 1998; Quirós & Justino, 2013) by enhancing the knowledge about internal certification drivers. Further, the study adds the new perspective of distinguishing between self- and third-party certification. From a practical perspective, it offers insights into potential advantages and downsides for companies that consider achieving certification according to the ISO 5230 standard. The study might support companies in their decision whether to strive for self- or third-party certification. Organizations maintaining ISO standards gain knowledge about what motivates companies to aim at ISO certification and what prevents them from doing so.

In the software supply chain, the role of OSS is increasing steadily and with it the topic OSS compliance (Morgan et al., 2013). Companies that do not fulfill the OSS license obligations face a significant risk of lawsuits against them, ultimately leading to substantial financial and reputational losses. Thus, the awareness of the necessity to adequately manage OSS compliance is growing constantly. Not only do companies increasingly care for their own OSS compliance, but also expect it from their suppliers. The topic is gaining relevance in supplier negotiations with customers asking for specific OSS compliance elements. However, there is not yet a common understanding across industries of what OSS compliance means and which measures need to be in place. Hence, managing OSS compliance when acquiring software with OSS components from external suppliers is especially challenging.

The recent ISO 5230 standard for OSS compliance and the respective certification should support software suppliers in credibly signaling their OSS compliance to their customers and other stakeholders. The question arises which role such a certification (self- vs third-party certification) plays for customer firms that select software suppliers compared to other selection criteria. Moreover, it is of interest whether potential decision-making patterns exist when selecting software suppliers to gain a more differentiated picture about the relevance of the different selection criteria for customer firms, including OSS compliance certification. These facts result in the following research objectives:

Research objective 3: Analyze the importance of OSS compliance certification (self- vs third-party certification) for customer firms in the software supplier selection process.

Research objective 4: Identify and characterize decision maker groups in the software supplier selection process and reveal factors that can predict group affiliation.

Research objective 3 is addressed in chapter 4, objective 4 in chapter 5. Both objectives fit to the open innovation process type “acquiring” in Dahlander and Gann’s taxonomy, as they take on the perspective of customer firms that select software suppliers.

The studies contribute to our theoretical understanding of the integration of OSS in commercial activities of companies. The literature on OSS certification is so far focused on certifying OSS itself, reflecting a strong product-focus (Feuser & Peleska, 2010; Kakarontzas et al., 2010). The approach examined in the studies in chapter 4 and 5 aims at certifying underlying OSS compliance processes instead, adding a new perspective to this literature stream. In IS research, the effect of software certifications has been investigated primarily in the B2C sector (Kaplan & Nieschwietz, 2003; Nöteberg et al., 2003). Research objectives 3 and 4 address the concept of compliance certification in the software supply chain and thus transfer the issue of certification to the B2B sector, more specifically to the OSS context. The studies also provide relevant implications for practitioners. They help software suppliers to decide whether OSS compliance certification is a signal they want to provide to their potential customers. Further, they provide support in the decision whether to strive for self- or third-party certification.

1.3 Research methods and designs

The research projects in this dissertation apply several different research methods, both qualitative and quantitative. In chapters 2 and 3, a multiple case study approach is adopted (Yin, 2009). This approach is considered most suitable to investigate recent phenomena, uncover relevant constructs and their relationships, and identify rationales and processes (Flick, 2022; Yin, 2009). Thus, this approach has been chosen to address research objectives 1 and 2. For chapter 2, several organizational units at Siemens AG serve as units of analysis to understand how companies accommodate organizational unit-specific requirements when designing OSS contribution governance processes. In chapter 3, the interview partners are grouped into self-certified companies, third-party certified companies, and third-party certification bodies to analyze differences in drivers, motives, and deterrents regarding OSS compliance certification. In both studies, interpretation of the data followed the thematic coding approach suggested by Flick (2022). In this approach, a deep analysis of each single case results in a system of categories that is elaborated further by applying open coding and selective coding (comparable to Strauss (1987)). A cross-check of the constructed categories leads to a thematic structure which serves as basis for the analysis and comparison of further cases.

In turn, for the research objectives 3 and 4, quantitative methods are applied. More specifically, for research objective 3, a discrete choice-based conjoint experiment is conducted (Louviere & Woodworth, 1983) to understand the relative importance of OSS compliance certification compared to other signals in the supplier selection process and to identify possible trade-offs. In the experiment, real-world software purchasing experts are asked to choose between offers from different software suppliers that all contain OSS components. The design of the conjoint experiment, specifically the selection of the decision criteria, is based on interviews with experts regularly involved in the selection of software suppliers. Compared to post hoc methods (e.g., interviews, surveys), conjoint experiments present certain advantages when investigating decision behavior. Post hoc methods rely on information from the past and thus might have to bear recall and rationalization biases (Zacharakis & Meyer, 2000). In contrast, conjoint experiments collect real-time information while decisions are made. Therefore, this method mimics the actual behavior of decision makers more accurately.

To address research objective 4, a two-stage cluster analysis, including hierarchical and non-hierarchical clustering approaches, appears to be the most suitable method. The sample consists of the decision makers participating in the conjoint experiment from chapter 4. The active clustering variables are the average utilities at the individual level of the supplier-related decision criteria from the previous conjoint experiment. The study first uses the single-linkage approach (to identify and eliminate outliers) and the Ward's minimum variance approach (to define the final number of clusters) as hierarchical clustering methods. In the second stage, K-means clustering is performed, which belongs to the non-hierarchical clustering methods, leading to the final cluster solution. The core benefit of this two-stage approach is the increase in validity of the final cluster solution, as it balances the downsides and biases of each single method (Everitt et al., 2011).

Subsequently, the relationship between the detected clusters and several individual, firm, and business until-level variables (passive variables) are analyzed in detail to identify factors that can predict cluster affiliation. Concretely, one-way analyses of variance (ANOVA) and post-hoc Tukey-Kramer tests are applied to examine whether the clusters depict statistically significant differences in the means of the passive variables of interest.

1.4 Structure of the dissertation

This dissertation comprises four studies. In the following, I briefly outline the structure of each chapter. Chapter 2 is titled “How companies govern their open source software contributions”. After introducing the study in chapter 2.1, the background section (chapter 2.2) relates the research objective to the IT governance literature and the literature on OSS governance from a community and company perspective. Chapter 2.3 gives detailed insights into the research context and explains the study design, data collection, and data analysis. Section 2.4 focuses on the results and describes how companies manage the trade-off between controlling their employees and granting them a certain degree of flexibility in their community engagement when designing certain OSS contribution governance mechanisms. The results are subsequently discussed under section 2.5. The chapter concludes by outlining implications for theory and practice (2.6) and by discussing limitations and possible areas for future research (2.7).

The title of chapter 3 is “Drivers and motives for open source software compliance certification in the software supply chain”. Following the introduction in section 3.1, chapter 3.2 defines OSS compliance and gives an overview of corresponding literature. Moreover, the OpenChain Project and the international standard for OSS compliance are introduced and motives for and deterrents to ISO certification already identified in literature are outlined. Chapter 3.3 focuses on the research method, describing the research design, sampling, data collection and analysis. The identified drivers, motives, and deterrents regarding OSS compliance certification are explained in detail under section 3.4. The findings are discussed in chapter 3.5, followed by practical and theoretical implications (3.6), limitations, and avenues for future research (3.7).

The study “The role of open source software compliance certification in the software supply chain – Insights from a conjoint experiment” is described in chapter 4. The chapter starts with an introduction (4.1) and subsequently reviews the literature on OSS certification and signaling theory (4.2). Section 4.3 focuses on the hypothesis development. The following chapter is dedicated to the research method, describing the research design, sampling, data collection, and potential biases related to data collection. The results are highlighted in section 4.5, followed by a thorough discussion (4.6). Again, the chapter concludes by mentioning implications (4.7), limitations, and avenues for future research (4.8).

Chapter 5 is closely related to the previous one, as it builds on the same sample. It is titled “Decision-making patterns in the selection of software suppliers”. Section 5.1 introduces the study, followed by the explanation of the clustering process and the subsequent analyses in the method section (5.2). The results, more specifically, the description of the final cluster solution, characterization of the different decision maker groups, and the identified predicting factors for group affiliation can be found in chapter 5.3. The study is complemented by a thorough discussion of the findings (5.4).

The final chapter 6 of this dissertation provides a summary of the results of the four studies. Further, it outlines the core theoretical contributions and points out the most relevant managerial implications.

2 How companies govern their open source software contributions[4]

2.1 Introduction

OSS has become increasingly important among companies (Ågerfalk & Fitzgerald, 2008; S. Y. Ho & Rai, 2017; Macredie & Mijinyawa, 2011; Rolandsson et al., 2011). Companies do not only passively use OSS, but they also need to actively contribute to it in order to implement specific functionalities and spread their standards. The active participation brings companies and OSS communities closer together and the interests of both parties must be met. Communities want to make sure that all participating parties comply with their requirements, whereas companies have to minimize the risk of inappropriate knowledge spillovers, protect company reputation, which may be hurt by low-quality contributions, and avoid violation of IP rights. Hence, the interaction requires governance of community as well as company activities. The existing literature addresses this phenomenon mainly by focusing exclusively on OSS governance from the community perspective (O'Mahony & Ferraro, 2007). This perspective has proved to be theoretically very insightful by showing how certain governance structures emerge in OSS communities and how they affect community members and outside parties.

From the company perspective, prior research has acknowledged the need for formalized instruments and processes on the company side to mitigate the risks associated with collaboration across companies and OSS communities (Germonprez et al., 2012). Yet, when introducing certain internal governance processes, companies face a significant trade-off. They need to ensure a compliant behavior towards the OSS communities and their environment in general, while enabling the organizational units, or more concretely their employees, to manage the specific contributions to OSS communities with a certain degree of flexibility.

Until now, the OSS contribution governance literature has paid little attention to this trade-off, which companies face when governing their employees who participate in OSS communities. The IT governance literature has already examined similar trade-offs

[4] This chapter is based on a paper co-authored by Michael A. Zaggl and Aron Lindberg. It won the "Student Paper Award for Best Industry Studies Paper" at the 53rd Hawaii International Conference on System Sciences (2020): Wissel, J., Zaggl, M., & Lindberg, A. (2020). Control vs Freedom: How Companies Manage Knowledge Sharing with Open Source Software Communities. Proceedings of the 53rd Hawaii International Conference on System Sciences.
Further, it has been presented at the International Conference on Information Systems (2019): Wissel, J., Zaggl, M., and Lindberg, A. (2019). How Companies Govern Their Open Source Software Contributions: A Case Study. ICIS 2019 Proceedings.

regarding the design of governance mechanisms. Yet, the focus strongly lies on companies' efforts to govern contributions from external parties to their own co-creation ecosystems (e.g., platform ecosystems) (Ghazawneh & Henfridsson, 2013; Svahn et al., 2017). Governing contributions from outside the company to own co-creation ecosystems can be described as outside-in perspective. It is highly relevant for companies that manage their own OSS projects. Yet, we lack insights into the mechanisms companies introduce to govern contributions from inside the company to OSS communities, which reflects the inside-out perspective.

Therefore, in this study, I aim at developing a new understanding of how companies design these mechanisms. More specifically, I want to find out how companies manage to control their employees while granting them a certain degree of flexibility in their community engagement. Hence, I ask the following research question: *How do companies negotiate the trade-off between control and flexibility regarding their employees' OSS community interaction?*

I approach this research question in a multiple case study (Yin, 2009) at Siemens AG with different organizational units as units of analysis. Siemens has recently set up a template OSS contribution process which the organizational units can adapt to their specific needs. Analyzing how the units adopt the template process and thereby define the flexibility for the developers offers the opportunity to find out how companies negotiate the tensions between control and flexibility by means of governance mechanisms.

Based on interviews with employees who work on OSS-related topics (e.g., software developers, experts for third party software, and managers) and archival data, I found that the extent to which the template process is implemented depends on the following characteristics of the organizational units: the level of closeness to core IP of the unit and the intensity of the involvement in OSS communities (i.e., number and type of contributions, number of OSS communities the unit is involved in). Moreover, I show that trust in the employees' technical skills and their OSS experience is essential for granting a certain flexibility for their engagement in OSS communities. Finally, in isolated cases where contributions happen very rarely and the closeness to core IP is low, developers set up a workaround instead of establishing a formal process.

This research contributes to the literature on company-involved OSS development (Ågerfalk & Fitzgerald, 2008; S. Y. Ho & Rai, 2017; Rolandsson et al., 2011), to the IT governance literature (Eaton et al., 2015; Ghazawneh & Henfridsson, 2013; Svahn et al., 2017; Wareham et al., 2014), and more concretely to the OSS contribution governance literature (Germonprez et al., 2017; Germonprez et al., 2012; O'Mahony & Ferraro, 2007) by showing how companies manage their employees' community interaction by means of governance mechanisms.

2.2 Background

2.2.1 IT governance

I draw on the definition of IT governance proposed by Gregory et al. (2018, p. 1227): "IT governance is defined as the decision rights and accountability framework deployed through a mix of structural, processual, and relational mechanisms and used to ensure the alignment of IT-related activities with the organization's strategy and objectives." This definition suits my research context very well, as it highlights the importance of processual mechanisms which are reflected in the template process introduced by Siemens.

Looking at the trade-off between control and flexibility, relevant studies in this literature stream have analyzed similar trade-offs that occur when implementing mechanisms to govern external parties' access to and participation in company-managed co-creation ecosystems (Eaton et al., 2015; Ghazawneh & Henfridsson, 2013; Svahn et al., 2017; Wareham et al., 2014). By doing so, companies maintain control over their ecosystems while at the same time allowing certain external contributions to develop them further.

Wareham et al. (2014), for example, examine a trade-off between control and autonomy in the context of technology ecosystems, which make use of many heterogeneous actors who engage out of self-interest in innovative activities. The authors find that the owners of technology ecosystems have to implement mechanisms to reduce variance to control low complement quality and to secure professional business conduct. At the same time, they have to make use of variance increasing mechanisms to guarantee a large high-quality portfolio of complements to stimulate user adoption (Wareham et al., 2014). Thus, companies must "establish governance mechanisms that appropriately bound participant behavior without excessively constraining the desired level of generativity" (Wareham et al., 2014, pp. 1195f.).

In addition, Svahn et al. (2017) analyze how incumbent companies can tackle competing concerns when driving forward their digital innovation efforts. One of the identified competing concerns for the Volvo Cars' Connected Car Initiative was control versus flexibility when it comes to innovation governance. When setting up a platform portfolio, Volvo Cars realized that they had to grant flexible access to in-car resources to foster external innovation. On the other hand, they had to implement certain control mechanisms to prevent unauthorized access from external parties (Svahn et al., 2017).

These two examples show that existing studies focus on the trade-off between control and flexibility companies face when setting up mechanisms to govern external access or contribution to own co-creation ecosystems. This outside-in perspective can be transferred to the OSS context as well, as an OSS community can be described as a co-creation ecosystem. Yet, it rather reflects the standpoint of OSS communities which introduce certain governance mechanisms to manage external contributions from their community members (also referred to as OSS governance). Literature has not yet dealt with the trade-off from an inside-out perspective, meaning the governance efforts companies take to manage their employees' contributions to OSS communities. Therefore, there is a need for developing an understanding of company governance mechanisms native to the company-OSS interface.

In this context, control through formal processes is necessary to secure high-quality contributions and prevent the violation from IP rights. At the same time, employees have to be granted a certain flexibility in their actions to stimulate the engagement with OSS communities, so that companies can influence to some extent the development of the corresponding OSS projects according to their needs.

2.2.2 OSS governance from the OSS community perspective

Each OSS project, regardless if it is collectively organized or managed by a company, relies on its specific community. In general, these OSS communities have two main groups of actors (Capra et al., 2009). The first group can be referred to as volunteers. They usually do not get any financial compensation for their contributions to OSS projects. Their motivation comes, for example, from the desire to improve their programming skills or to create a specific functionality in the code needed for their non-work life (Lakhani & Wolf, 2003). Companies that pursue various technical and business interests through their participation in OSS projects build the second group of actors. Many developers are employed by a company and paid for their engagement with specific OSS communities. Possible ways of engaging are the development of concrete software components according to their company's requirements, the removal of bugs, or creating documentation (Capra et al., 2009). In this study, I mainly talk about OSS communities, as I focus on the actors behind the OSS project rather than the technical project itself.

The interaction of companies and OSS communities requires governance mechanisms from both parties to secure their interests. The definition of OSS governance as “the means of achieving the direction, control, and coordination of wholly or partially autonomous individuals and organizations on behalf of an OSS development project to which they jointly contribute” by Markus (2007, p. 152) refers to governance mechanisms coming from the side of the OSS community. In this research stream, which focuses on the community perspective, scholars examined different aspects related to OSS governance. Some examples are structures of roles and responsibilities (Mockus et al., 2002), formal and informal rules inside communities (e.g., verifying developer identity, according developer status to new members) (Krogh et al., 2003; O'Mahony & Ferraro, 2007), and the relationships between companies and OSS communities (Dahlander & Magnusson, 2005).

2.2.3 OSS governance from the company perspective

From the company perspective, the existing literature provides insights into how companies react to market decisions, intertwined ideologies, and distributed connections among OSS community members (Germonprez et al., 2017; Germonprez et al., 2012). As an example, Germonprez et al. (2017) developed the theory of responsive design as a special form of corporate software design. This approach extends the traditional corporate software design approach. Instead of relying on a team of internal developers solving a specific problem, company-involved OSS development is characterized by a dynamic variety of activities and intensive interaction with the OSS communities.

Further, prior research has shown the relevance of formal governance processes introduced by companies to govern their employees’ contributions to OSS communities (Germonprez et al., 2012). Apart from software scanning and exchanging open source data between companies, governance processes set up by internal open source program offices to secure the protection of IP and license compliance are seen as the primary risk mitigation options. Thereby, the processes help to mitigate the risks which accompany the interaction with these communities (Germonprez et al., 2017; Germonprez et al., 2012). Yet, so far it has not been examined how companies design these processes to negotiate the tensions between controlling their employees and granting a certain degree of flexibility in their interaction with OSS communities.

To clearly differentiate the governance processes set up inside companies from those related to the governance of OSS communities (according to the definition of OSS governance), I introduce the term *OSS contribution governance*. This term refers to the processes companies implement to govern their employees’ engagement in OSS communities.

2.3 Method

2.3.1 Research context and design

To address the research question, I adopt a multiple case study approach with different organizational units as units of analysis (Yin, 2009). I consider this approach as most suitable for this research, as the aim is to analyze how each unit manages the trade-off between control and flexibility regarding their employees’ OSS community interaction.

My research context is Siemens AG, a German multinational conglomerate company with headquarters in Munich and Berlin. With about 379,000 employees worldwide and a revenue of €83.0 billion in 2018, Siemens is one of the largest producers of industrial technologies. The company is a leading supplier of power generation and transmission systems and medical diagnosis as well as infrastructure and industry solutions. This portfolio reflects a large diversity of B2B products, systems, and solutions. In almost all of the areas Siemens is active in software is of paramount importance. Below the Group level, there are three Operating Companies and three Strategic Companies reflecting the core businesses. Each of the Operating and Strategic Companies is divided into different business units. They are supported by the corporate units from Corporate Development and the Service Companies, which all provide cross-divisional functions across whole Siemens.

Siemens is suitable for this study for two reasons. First, OSS is a highly relevant topic in many Siemens units. The quantity of OSS components used in Siemens products is increasing steadily and the awareness for an active engagement with OSS communities is rising among Siemens employees. The number of commits on GitHub by Siemens employees increased from 345 commits in 2011 to over 21,000 commits in 2018. Second, the organizational units of Siemens possess a large degree of autonomy. They use OSS to varying extents and for different purposes. Hence, different requirements regarding the governance mechanisms apply within the company.

Siemens has recently set up a template OSS contribution process to govern their employees who interact with OSS communities. It secures that the employees in the organizational units comply with external regulations as well as community norms, which is essential for a positive perception of Siemens as a whole, from the perspective of its stakeholders. The template process, in its original version, is quite complex, which results in a low degree of flexibility for the developers in their interaction with OSS communities. Each organizational unit can decide to adopt the whole process or a modified version of the process or to stick to the already existing procedures, as “dictating a process is always difficult" (ETPS1). Analyzing how the organizational units adapt the process to their specific needs and thereby define the flexibility for the developers opens up the opportunity to find out how companies negotiate the trade-off between control and flexibility by means of governance mechanisms.

2.3.1.1 Development of the template OSS contribution process

In the second half of 2017, the need for a Siemens-wide template OSS contribution process came up in the *Open Source Task Force*. This task force aims at connecting all organizational units at Siemens, which deal with OSS, to give them the opportunity to discuss OSS-related topics and exchange experiences:

> "This was a topic which popped up after all other topics were handled slowly but surely. How is the clearing to be done, how is everything archived, how is the delivery to be done, etc."[5] (ETPS2)

Besides representatives from the legal and the IP department, strategic procurement, and internal IT, the *experts for third party software* of each organizational unit are members of the task force. Each organizational unit has a designated *expert for third party software*, who secures that an adequate product clearing is performed to guarantee that third party software components, including OSS, are used according to the license terms. The main reasons for setting up a Siemens-wide template OSS contribution process were: (1) to protect employees as well as Siemens' business interests and reputation, (2) to comply with legal and internal regulations, (3) to provide transparency to decision makers regarding the effect of the contribution on Siemens' code and IP, and (4) to adhere to the rules and customs of the OSS ecosystem.

The template OSS contribution process was derived from an already existing tool-supported approval process for publications (e.g., conference papers and journal publications). Corporate unit 1, more specifically the team responsible for Siemens-wide OSS-related topics, took the leading role in the development of the template process, as they had already designed a contribution process for their specific unit based on the publication approval process:

> *"[In our unit,] we already have an OSS contribution process for a long time and we brought it into the discussion with the task force as it was already tool-supported. [...] We took the opportunity to say, okay, let's sit together and design a process that can be used as template process."*[5] (ETPS1)

[5] Quote translated from German to English by the author.

The tool support facilitates identification of persons responsible to be involved in the respective process and documentation of process outcomes. The already existing process for publication approval was adapted to the requirements of OSS contributions.

2.3.1.2 Description of the template OSS contribution process

Figure 2-1 represents the Siemens-internal visualization of the central template OSS contribution process. The process is split into two parts. The first part is development-related, the second one refers to the different actors necessary for approval. The development-related part represents the steps of the process with active engagement of the developer (i.e., *Siemens contributor*).

As a first step, the contributor needs to ensure that the source code is clean and ready for contribution. This includes a review of the code by an experienced peer developer. Subsequently, the contributor has to provide the following information via the publication approval tool: (1) Name and URL of the OSS project, (2) license of the project, (3) contribution policy of the project (e.g., possible contributor license agreement (CLA) or developer certificate of origin (DCO)), (4) context in which the code was developed, and (5) cleaned source code.

In a next step, the *expert for third party software* of the corresponding organizational unit and the technical manager (i.e., usually the line manager) are informed automatically via the tool that their participation is required in the new workflow. The technical manager has to confirm that he obtained the permission to contribute from the budget owner of the project in which the code has been developed. If the contribution aims at a crypto library, the technical manager also has to consult the department for export control and customs. In case of unclear license terms of the OSS project or the requirement of an unknown CLA or DCO, the *expert for third party software* involves the legal department. The IP department is consulted by default to ensure that no IP is affected by the contribution. In general, two forms of company expertise are involved in the process: legal expertise and technical expertise. If all parties involved give their permission, the approver (i.e., a person with the power to sign in the name of Siemens) gives the final permission to contribute and signs the CLA, if necessary. If one of the required permissions is not given, the contribution request is rejected. In its original version, the template process is mandatory for every planned contribution to OSS communities.

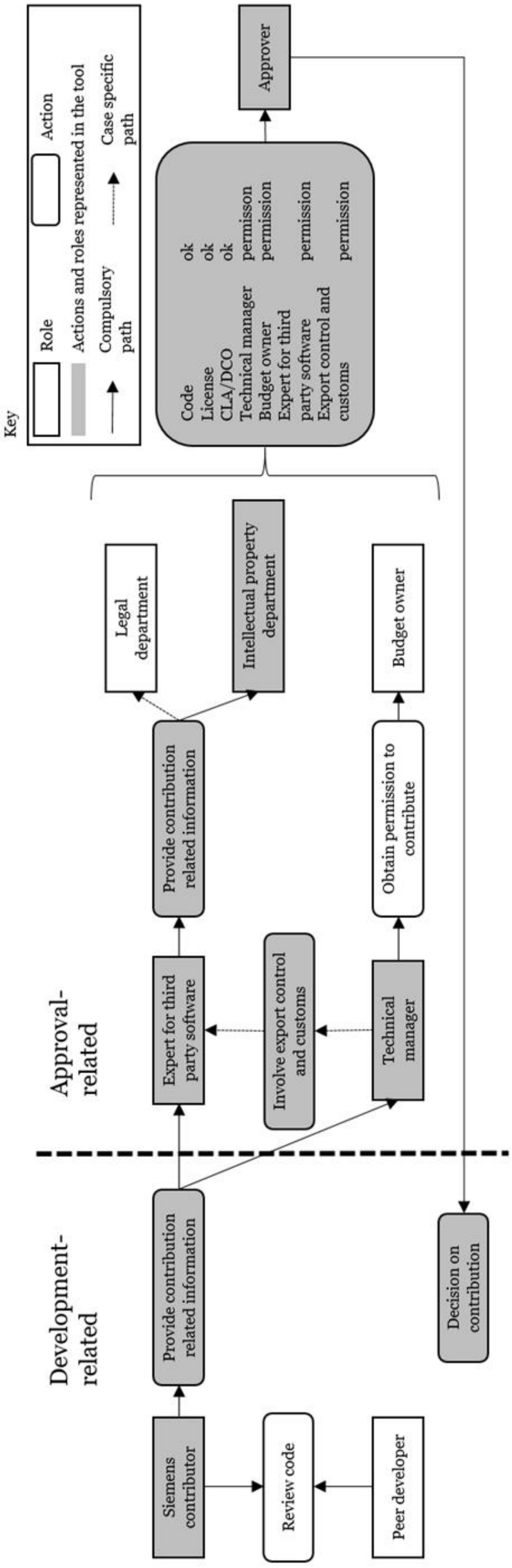

Development-related
Approval-related
Siemens contributor
Review code
Peer developer
Provide contribution related information
Decision on contribution
Expert for third party software
Involve export control and customs
Technical manager
Provide contribution related information
Obtain permission to contribute
Legal department
Intellectual property department
Budget owner
Code ok
License ok
CLA/DCO ok
Technical manager permisson
Budget owner permission
Expert for third party software permission
Export control and customs permission
Approver
Key
Role
Action
Actions and roles represented in the tool
Compulsory path
Case specific path

Figure 2-1: Siemens-wide template OSS contribution process

2.3.2 Data collection

To get a deeper understanding of the phenomenon and related real-life practices, I collected qualitative data. To achieve triangulation (Yin, 2009), I collected data from various sources: semi-structured interviews, internal documentation, and direct observations during OSS-related meetings and a company visit. Internal documentation included wiki entries, process descriptions and visualizations, and checklists. I conducted twelve interviews over a six-month period with software developers and architects dealing with OSS, experts for third party software, and managers involved in OSS-related decision-making. The interviewees represent two business units and one corporate unit. Table 2-1 summarizes the interviewee profiles.

The interviews were guided by a semi-structured protocol, which was designed prior to data collection according to the research question. It was adapted to the characteristics of the interviewees and insights from previous interviews. The protocol consisted of three parts, which I defined in advance to ensure comparability of the responses (Flick, 2022). As an introduction, the interviewees were asked for a description of their organizational unit, their personal role, and main responsibilities. The second part dealt with the role of OSS for the respective unit (e.g., attitude towards OSS, ways of using OSS, engagement with OSS communities). The last part covered questions about how OSS contributions are managed (e.g., description and assessment of processes, reasons for chosen process design). All interviews were audio-recorded with the permission of the respondents and transcribed verbatim. Each interview lasted between 30 and 70 minutes, resulting in about 10.5 hours of recording. The interviews were conducted in English and German. Quotes from interviews conducted in German were translated into English by me and are marked accordingly.

Table 2-1: Summary of interviewee profiles

Organizational Unit	Description	Interviewees
Corporate Unit 1 (CU1)	Central research and development unit which provides cross-divisional services along the entire value chain to the business units	Expert for third party software (ETPS1) Research scientist OSS (RS1) Open source expert (OSE1) Open source expert (OSE2) Software developer (SD1) Software developer (SD2)
Business Unit 1 (BU1)	Provides products, systems, and solutions for a reliable transmission and distribution of electrical energy	Expert for third party software (ETPS2) Software architect (SA1) Software developer (SD3)

Organizational Unit	Description	Interviewees
Business Unit 2 (BU2)	Provides motion control systems and solutions for production and tooling machines	Expert for third party software (ETPS3) Software developer (SD4) Software developer (SD5)

2.3.3 Data analysis

First, I developed a deep understanding of the template process, mainly based on internal documentation and narratives. During a company visit, two company representatives from the team responsible for Siemens-wide OSS-related topics, which is located in CU1, gave a detailed description of the template process, especially its evolution and characteristics. Moreover, they provided internal documentation related to the template process (e.g., presentations, guidelines, wiki entries). This was an essential step to be able to analyze subsequently to what extent this process has been adopted in different organizational units and which specific characteristics influence the process design and thus the degree of flexibility for the developers.

The prevailing data source in the main step of the analysis were the interviews with employees from different organizational units. I analyzed the data using MAXQDA, a software for qualitative data and text analysis. The coding process followed a thematic coding approach (Flick, 2022). This approach has been developed to investigate the spread of perspectives on a phenomenon or a process. It fits the aim of this research, as I want to find out how different organizational units negotiate the trade-off between control and flexibility regarding their employees' OSS community interaction by means of governance mechanisms. In a first step, I looked at each unit separately and developed detailed case descriptions. The focus lay on the relation with and handling of OSS, the OSS contribution process, and the reasons why the unit chose the specific process design. As a result of this step, a system of thematic domains and categories evolved for each single case by applying open and selective coding (Flick, 2022; Strauss, 1987). Subsequently, a thematic structure was developed which was constantly adjusted when new factors emerged during the analysis of the different cases. Finally, the thematic structure was used to compare the different organizational units (Flick, 2022).

2.4 Findings

In my analysis, I identified two key dimensions which influence the decision to what extent the template process is implemented and thus the resulting degree of flexibility for the developers. Both dimensions represent specific characteristics of the organizational units. First, it plays a role how close the unit is to core IP. If the unit deals with highly sensitive IP-related topics, the risk of revealing confidential information is higher. Hence, the process tends to be stricter, resulting in a low degree of flexibility.

The second dimension is the intensity of the unit’s involvement in OSS communities (i.e., number and type of contributions, number of OSS communities the unit is involved in). For a low intensity of involvement, I observe two possible effects: First, it can lead to a stricter process and thus a higher flexibility, as checking only few OSS contributions is still easily manageable with the available resources. The second possibility is that units do not recognize the need for formal processes due to the low number of contributions. With an increasing intensity of involvement, I find that trust in the developers’ technical skills and the experience in the interaction with OSS communities gains importance. As soon as the number of contributions exceeds the process capacity, units have to find solutions to increase the developers’ flexibility.

In the following, I describe the various process adoption approaches across the investigated corporate and business units, reflecting different degrees of flexibility for the developers. Table 2-2 summarizes the different approaches.

Table 2-2: Comparison of process adoption approaches

		Intensity of involvement in OSS communities of the organizational unit	
		Low	High
Level of closeness to core IP of the organizational unit	Low	No adoption of the template process (workaround established)	Adoption of the template process with modifications
			No adoption of the template process (rely on existing process)
	High	Full adoption of the template process	-

In the case of a strong closeness to core IP of the organizational unit and a low intensity of involvement in OSS communities, the template process was fully adopted. One example is BU1. Before the process implementation, BU1 was not contributing back to OSS communities and there was little experience in the company-community interaction. It was only when two developers with the intention to contribute actively approached the respective *expert for third party software* that the need for a process arose:

> *“I pushed [the development of the template process] actively, as we had two colleagues who desperately wanted to [contribute code].”*[5] (ETPS2)

BU1 deals with critical infrastructure for energy supply and thus is close to core IP. Developments in this area have to be protected and hence are not intended to be made open source:

> *“When it comes to functionalities, you always have to discuss. IP is always an issue. […] We always have to consider what is core know-how and has to be protected.”*[5] (SA1)

Since the process implementation, employees only made two contributions in the form of bug fixes to two different OSS projects, indicating a low intensity of involvement in OSS communities. BU1 fully adopted the template process, resulting in a low flexibility for the developers, as each contribution has to undergo the process:

> *“In principle, every change needs to go through [the process]. […] Should something appear again, same developer, same component, then we might think about shortening it a bit.”*[5] (ETPS2)

For organizational units characterized by a low level of closeness to core IP and a high intensity of involvement in OSS communities, I find two possible outcomes. First, the template process was adopted with certain modifications. One example is CU1. In this unit, many developers are actively involved in several different OSS projects. Contributions comprise different types, including feature enhancements. These facts underline a high intensity of involvement in OSS communities. Employees consider the risk to reveal IP relevant information to OSS communities as comparably low. CU1 decided to largely adopt the template OSS contribution process. Yet, not every single contribution can undergo the process, as its capacity is limited and the highly dynamic OSS environment oftentimes requires rapid actions. Thus, developers are granted certain facilitations, which range up to general approvals for specific OSS projects. This means that the developers have to undergo the process only once when asking for approval to engage actively in a certain OSS project under specified conditions (e.g., under a specific license). This facilitation reduces the effort not only for the developers but also for all other persons involved in the contribution process:

> *“If you are seriously dealing with OSS, […] you have to find a way which is legally and practically feasible. This means enabling the daily work without leaving the legal framework.”* (SD1)

Further, more flexibility for the developers in their interaction with OSS communities is achieved. These general approvals require a certain amount of trust in the developers that they do not leave the set scope of action:

> *“[The process] comes along with the trust that you as a developer stay in this framework.”* (SD1)

Hence, it is only granted to senior developers who have already demonstrated both their technical skills and their ability to interact with the target OSS communities according to their rules and practices.

The second outcome for this configuration is that the respective organizational unit sticks to an already existing process instead of adopting the template process. One example is BU2. In this unit, an established OSS contribution process exists, yet not tool-supported. This process is embedded in the product lifecycle management process of BU2. If developers want to make a contribution, they have to fill out the publication request for OSS. This document comprises information about the development context, the OSS itself, and a checklist with the main concerns developers have to consider when planning a contribution. The completed form has to be signed by the *expert for third party software* and a person with the power to sign in the name of Siemens to get the permission to contribute. The permission can also be granted on project level, similar to the facilitation introduced by CU1. Apart from the missing tool support, the process shows many similarities with the template process. However, it seems to be less complex due to the smaller number of persons involved. The reduced effort and resulting flexibility are highly appreciated by those teams of the unit who make several contributions per day during critical development phases, ranging from bug fixes to feature enhancements:

> *"[The general approval] was very important for me. If I do several patches a day in a critical development phase, I don't want to pass multiple hierarchy levels each time to get a permission from someone who most likely cannot evaluate technically what is going on."* (SD4)

The fact that the above-mentioned form was only filled out three times in the last seven years reflects a generally low willingness to contribute in BU2. However, it cannot be completely ruled out that contributions are made without adhering to the process. A team with a low intensity of involvement in OSS communities in the same organizational unit established a workaround. An agreement was made between the superiors and the developers which allows them to contribute bug fixes under the personal identity and not on behalf of Siemens, resulting in a high flexibility for the developers. This procedure was established about 12 years ago when there was no experience with OSS contributions yet to avoid the need to establish a formal process:

> *"At that time, there were definitely reservations [about OSS], we didn't know how we would do [contributions]. We agreed that if [the contribution] really does important things, I can do it under my private name instead of contributing it officially in the name of Siemens. In those days, this was the easiest resort without having to set up formal processes."* (SD5)

The effort to create an OSS contribution process was considered as too high compared to the benefit of the contributions. This agreement is still valid today and there are no endeavors to change the procedure so that a small number of contributions stays under the radar.

2.5 Discussion

The analysis of the OSS contribution processes in different organizational units at Siemens has shown that two key dimensions determine the decision to what extent the template process is implemented. The resulting process ultimately also defines the degree of flexibility for the employees who interact with OSS communities. The first dimension is the closeness to core IP of the organizational unit. Scholars have recognized the protection of IP as one of the main concerns companies have to deal with when interacting with OSS communities (Germonprez et al., 2012). Companies face the risk of unintentionally releasing IP to OSS communities because of licensing requirements (McGhee, 2007). Hence, my finding that the closeness to core IP is a decisive factor for how companies design mechanisms to govern their employees' engagement with OSS communities is supported by the existing literature.

The second dimension I find is the unit's intensity of involvement in OSS communities. Prior research has shown that the degree of participation in OSS communities is decisive for understanding how companies make use of the work of OSS communities (Dahlander, 2007). Companies use to become engaged with communities which they consider as highly relevant software modules for their products. I observe that a low involvement in OSS communities can lead to two extreme outcomes regarding the OSS contribution process design: the implementation of a very strict process (resulting in low flexibility) or no formal process at all (with a workaround instead). When looking for an explanation for the different outcomes, the first dimension comes into play. A high closeness to core IP combined with little experience in OSS community engagement drives units to be more cautious and thus to implement stricter processes with less flexibility for the developers. In contrast, for units which are not dealing with IP-related issues, the need for formal processes to manage their low OSS community involvement does not become apparent.

With an increasing intensity of involvement, one might also expect a stricter process to ensure that the multitude of contributions complies with internal regulations and is of high quality. Yet, I find that as soon as the number of contributions is not manageable anymore via a strict process, units have to find solutions to increase the developers' flexibility. Thus, trust in the developers' technical skills and the experience in the interaction with OSS communities becomes increasingly important.

To summarize, in this study I find that the two above-mentioned key dimensions are decisive for how companies design their OSS contribution processes and thereby manage the trade-off between control and flexibility when governing their employees in their interaction with OSS communities.

2.6 Implications for theory and practice

The study contributes to several literature streams. First, it contributes to the literature on company-involved OSS development (Ågerfalk & Fitzgerald, 2008; S. Y. Ho & Rai, 2017; Macredie & Mijinyawa, 2011; Rolandsson et al., 2011). This multiple case study provides new insights into how companies manage their interaction with OSS communities and how they do justice to the fact that their different organizational units have specific needs regarding their OSS community engagement. In addition, it contributes to the IT governance literature (Eaton et al., 2015; Ghazawneh & Henfridsson, 2013; Svahn et al., 2017; Wareham et al., 2014) and more concretely to literature on OSS contribution governance (Germonprez et al., 2017; Germonprez et al., 2012; O'Mahony & Ferraro, 2007). So far, scholars have mainly focused on the trade-off between control and flexibility that occur when implementing mechanisms to govern external parties' access to and participation in own co-creation ecosystems (outside-in perspective). I add the inside-out perspective and provide insights into how companies manage this trade-off when governing their employees' OSS community engagement.

The insights from my study also provide valuable recommendations for practitioners. First, providing flexibility to the organizational units in adopting contribution processes to accommodate their specifics is essential for companies. Simply dictating a process might decrease the employees' willingness and ability to engage with OSS communities. Hence, companies might profit less from the involvement, as they are not able to keep up with the fast OSS environment anymore. Second, granting developers particular facilitations based on technical skills and the experience in interacting with OSS communities is a suitable way to provide each of them individually with a certain degree of flexibility in their community engagement.

2.7 Limitations and avenues for future research

I have specifically chosen various organizational units at Siemens for my multiple case study, as OSS plays a significant role for the company as a whole, whereas each unit deals with it differently. However, the fact that I focused on units in one single company challenges the validity of the findings. Therefore, the topic should be investigated in further companies with differing characteristics (e.g., size, industry, location). This would also help to strengthen the finding of this study that the two key dimensions are really the most important factors when companies decide about the governance processes related to their employees' OSS community engagement. Although one could think of further aspects influencing a company's decision between control and flexibility with regard to the OSS contribution process design (e.g., business model, maturity of the software), they did not become apparent in my multiple case study at Siemens.

Moreover, the insights from this study are highly context-specific, meaning that they apply for companies that interact with OSS communities. Thus, it would be worth looking at contexts which involve other co-creation ecosystems (e.g., platform ecosystems) to find out if the findings match.

Finally, investigating further organizational units, especially those with a high level of closeness to core IP and high intensity of involvement in OSS communities, would help to get an even broader view on the process adoption approaches. I am lacking observations for this specific configuration. One reason could be that only few (or even no) organizational units exist that have a strong closeness to core IP and are still highly involved with OSS communities, as the fear of unintendedly disclosing core IP prevails.

3 Drivers and motives for open source software compliance certification in the software supply chain

3.1 Introduction

The increasing importance of OSS for companies leads to significant entanglement of OSS communities, companies, and providers of OSS (Ågerfalk & Fitzgerald, 2008; S. L. Daniel et al., 2018; Macredie & Mijinyawa, 2011; Medappa & Srivastava, 2020; Stewart et al., 2006). This development makes the compliance of companies with OSS principles an increasingly relevant topic (Morgan et al., 2013). Compliance refers to OSS users, integrators, and developers respecting copyright notices and abiding by obligations that come along with the different OSS licenses (Haddad, 2016). Companies insufficiently managing their OSS compliance risk violating license terms, which can result in litigations, leading to significant financial and reputational losses for companies (Harutyunyan, 2020). Managing compliance is especially difficult when companies acquire OSS components from external software suppliers.

In 2020, a new ISO standard (ISO/IEC 5230) has been published to facilitate OSS compliance. It defines the core measures for OSS compliance and makes it possible to ensure compliance. Based on this standard, companies can achieve a self-certification or third-party certification (The Linux Foundation, 2022). For self-certification, companies can fill in an online questionnaire and upload documentation as evidence for fulfilling the essential criteria for being OSS compliant. Alternatively, companies also have the option to be certified by different third-party certification bodies. In the software supply chain, this certification is supposed to help software suppliers in credibly demonstrating their OSS compliance to their customers and other stakeholders.

While literature has already examined motives and deterrents regarding several established ISO standards (e.g., ISO 9000) (Anderson et al., 1999; Quirós & Justino, 2013), ISO 5230 is a relatively new standard. Moreover, it has the rather unique characteristic that apart from third-party certification, also self-certification can be pursued. This fact points at potentially differing motives and deterrents for the two certification approaches. Hence, this study aims at answering the following research questions: *Which drivers for OSS compliance certification exist? What motivates or prevents companies from attaining OSS compliance certification (self-certification or third-party certification)?*

I conduct a multiple case study based on the thematic coding procedure introduced by Flick (2022). In total, 17 semi-structured interviews were conducted with representatives from companies that were either self-certified or certified by a third party and with representatives from third-party certification bodies that offer OSS compliance certification.

Results show that customers appear to be the largest external driver for self-certified and third-party certified companies. Certification bodies regard regulation as most relevant driver. From an internal perspective, the increasing relevance of OSS for companies is the most decisive driver for all three groups. Regarding general motives for OSS compliance certification, all three groups name the ability to use it as evidence for OSS compliance in negotiations as most decisive factor. Self- and third-party certified companies thereby mostly refer to negotiations with customers, whereas certification bodies focus on acquisition scenarios. When it comes to specific motives for self-certification, using the ISO standard as benchmark was mentioned most frequently, mostly to cross-check existing OSS compliance processes, but also to design processes from scratch. The most relevant motive for third-party certification across all three groups is the unbiased assessment of OSS compliance by an independent third party. Finally, the generic nature of the ISO standard is not only perceived as advantage, but also as downside. Due to the general formulation, firms sometimes struggle to translate the standard into working processes and certifiers lack guidance regarding which processes to consider as certifiable.

With this study, I contribute to the literature on ISO certification (Anderson et al., 1999; T. Y. Lee, 1998; Quirós & Justino, 2013) by adding significant insights on internal certification drivers. In the case of ISO 5230 certification, committed employees and the increasing relevance of the topic OSS compliance for companies make companies seek certification. Further, I add the new perspective of distinguishing between self-certification and third-party certification. Using the ISO standard as benchmark, the equal perception of self- and third-party certification, as well as the availability of the necessary competencies inside the company stand out as relevant motives for self-certification. In contrast, the assessment of OSS compliance measures by an independent third party is the most important factor speaking for third-party certification.

This study also provides several practical implications. For companies that think about achieving certification according to the ISO 5230 standard, it offers insights into potential advantages and downsides. The study might support companies in their decision whether to strive for self- or third-party certification. Organizations maintaining ISO standards gain knowledge about what motivates companies to aim at ISO certification and what prevents them from doing so. Moreover, they should take into account the ambiguous perception of the generic nature of most ISO standards and provide companies with additional material to allow them to design adequate processes that comply with the standard.

3.2 Background

3.2.1 OSS compliance

This study draws on the definition of OSS compliance introduced by Koltun (2011, p. 95): OSS compliance “refers to the aggregate of policies, processes, training, and tools that enables a company to effectively use FOSS (…), while respecting copyrights, complying with license obligations, and protecting the company’s IP and that of its customers and suppliers”.

While the nature of OSS allows the source code to be freely accessed, modified, and distributed by anyone, OSS adoption indeed comes along with certain obligations that result from specific OSS licenses (Riehle & Harutyunyan, 2019; Välimäki, 2005). So far, the Open Source Initiative has approved 117 different OSS licenses, all varying in their restrictiveness[6]. Figure 3-1 illustrates the five most common software license categories.

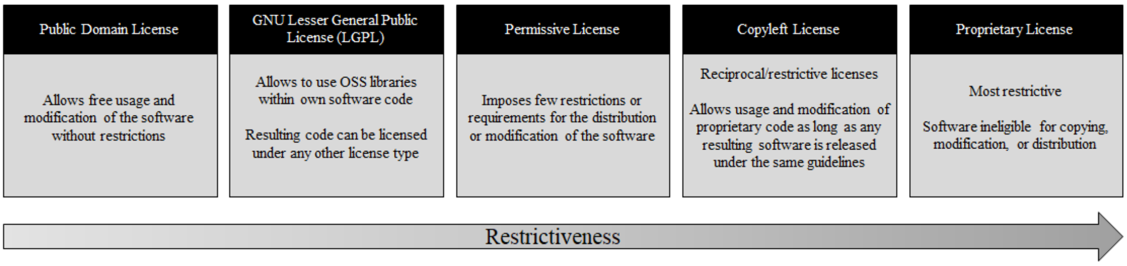

Public Domain License
Allows free usage and modification of the software without restrictions
GNU Lesser General Public License (LGPL)
Allows to use OSS libraries within own software code
Resulting code can be licensed under any other license type
Permissive License
Imposes few restrictions or requirements for the distribution or modification of the software
Copyleft License
Reciprocal/restrictive licenses
Allows usage and modification of proprietary code as long as any resulting software is released under the same guidelines
Proprietary License
Most restrictive
Software ineligible for copying, modification, or distribution
Restrictiveness

Figure 3-1: Most common software license categories[7]

The ignorance concerning licenses, insufficient documentation, and increasingly complex IT processes inside companies drive the risk for violating OSS license requirements (Gangadharan et al., 2012; Riehle & Harutyunyan, 2019; Yun et al., 2017). Violating license requirements can result in litigations, leading to significant financial and reputational losses for companies. Thus, defining adequate rules and processes for OSS adoption are crucial to mitigate the associated risks. The topic OSS compliance is gaining relevance across all industries. However, many companies are still not aware of

[6] According to https://opensource.org/licenses/, retrieved June 5, 2023
[7] Based on https://snyk.io/learn/what-is-a-software-license/, retrieved June 28, 2023

the risks related to lacking OSS compliance and have not yet implemented adequate measures to ensure being compliant (German & Di Penta, 2012).

3.2.2 The OpenChain Project and the international standard for OSS compliance

In 2016, the OpenChain Project was founded with the goal to develop a common understanding of OSS compliance. The project is hosted by the Linux Foundation. It aims to increase trust in the software supply chain, which increasingly contains OSS components. In the OpenChain Project, thousands of companies worldwide collaborate to increase the speed and effectiveness of the supply chain by standardizing OSS compliance (The Linux Foundation, 2022). Standardizing OSS compliance processes helps companies to comply with the obligations and regulations of OSS licenses. Further, they support the effective use of OSS components in their own products, the compliance with obligations resulting from contracts with software suppliers, and the protection of proprietary IP (Haddad, 2016).

One major achievement of the OpenChain Project is the development and maintenance of the international standard for OSS compliance. It is suitable for any type of company across all industries, independent of the position in the supply chain. The standard defines the core elements of a thorough OSS compliance program, such as a documented OSS policy, clearly defined roles and responsibilities regarding OSS compliance, and being able to provide a software bill of materials (SBOM) including all OSS components. The standard has been approved as the official ISO standard ISO/IEC 5230[8] at the end of 2020.

Based on this standard, two approaches exist for companies to demonstrate OSS compliance. First, the OpenChain Project offers a self-certification free of charge. By filling in an online questionnaire and providing certain verification material, companies can show that they fulfill the criteria set for being OSS compliant. Alternatively, companies have the option to be certified by third-party certification bodies (The Linux Foundation, 2022), which involves significant costs. In Germany, this certification is offered, for example, by PricewaterhouseCoopers GmbH and TÜV Süd AG.

[8] Current version of the ISO/IEC 5230 standard: https://standards.iso.org/ittf/PubliclyAvailableStandards/c081039_ISO_IEC_5230_2020(E).zip

3.2.3 Motives for and deterrents to ISO certification

To gain a comprehensive picture on drivers and motives for ISO certification, it is worth looking into further literature streams beyond the software context. Literature so far has identified several internal and external motivational factors for ISO certification, especially for ISO 9000, a set of five quality management systems standards that support companies in meeting their stakeholders' needs within legal and regulatory requirements linked to a product or service. Yet, results are oftentimes inconclusive (Corbett & Kirsch, 2001). Anderson et al. (1999) summarized reasons for companies to (not) pursue an ISO 9000 certification. They found the fulfillment of regulation and customer requirements and the prospect of a competitive advantage to be important external motivational factors. As customers tend to associate ISO certification with high quality, many companies see the potential to create a positive public image and to increase their stakeholders' trust (Boiral, 2012; Pekovic, 2010). This results in the risk of firms seeking ISO 9000 certification only for marketing reasons, not to achieve actual product or process improvements (van der Pijl et al., 1997). Finally, the potential to increase sales or market share has been identified as important external certification motive. For companies, ISO 9000 certification can facilitate the expansion to new markets, the access to further customer segments, or the sales increase in existing markets (Anderson et al., 1999; Quirós & Justino, 2013; Terziovski et al., 1997).

From an internal perspective, seeking process and quality improvements, cost reductions, and an increase in transparency were identified as relevant factors (Anderson et al., 1999). A study by T. Y. Lee (1998) on ISO 9000 certified companies in Hong Kong found similar results, highlighting that motivations differ across industries and firm sizes. Brown et al. (1998) discovered that internal motivational factors (e.g., cost reductions, quality improvements) were less important than external ones (e.g., customer requirements). In contrast, a survey among certified companies in the U.S. revealed that quality improvements and customer requirements were mentioned equally often as most decisive motive for ISO 9000 certification. 95.2% of the respondents observed internal benefits resulting from the certification, compared to 85.4% who observed external benefits (Irwin, 1996). Due to these inconclusive results, drawing conclusions about the relative importance of the different factors is difficult.

Anderson et al. (1999) also disclosed several deterrents to ISO 9000 certification. One is the existence of better (and less costly) alternatives to comply with regulations and procurement standards and to disclose quality information. In addition, the cost of certification plays a significant role, especially for smaller firms and those with a low level of maturity of their initial quality control measures. Finally, a potential competitive disadvantage through a premature technology lock-in might prevent companies from seeking ISO 9000 certification, in particular in highly agile environments (Anderson et al., 1999).

3.3 Method

3.3.1 Research design, sampling, and data collection

This study applies the comparative case study approach by Flick (2022). It is based on the comparative case study approach by Strauss (1987), with the difference that the groups to be studied are defined in advance instead of resulting from the state of interpretation. The underlying assumption in Flick's approach is that different groups have different views on the phenomenon under study. Aim of the approach is to develop a deep understanding of the opinions and experiences of each group under study and to compare them. Sampling should focus on those groups that are expected to deliver the most informative insights to answer the research questions (Flick, 2022). This procedure matches well the phenomenon examined in this study. The view on OSS compliance certification is expected to differ for self-certified and third-party certified companies, as well as for third-party certification bodies. Thus, these three groups need to be looked at separately. In each group, theoretical sampling was conducted to select the specific cases to be studied.

First, companies had to be identified that fit one of the three groups under study. The main source was the homepage of the OpenChain Project, on which many companies announced their certification according to the ISO 5230 standard. Possible interview partners in suitable companies were then identified via a manual LinkedIn search for experts in the area of OSS compliance or third-party software license management. In addition, personal contacts to OpenChain representatives and a call for participation via the OpenChain mailing list were used to attract interview partners. Table 3-1 gives an overview of the interviewees.

The focus of data collection should lie on ensuring data comparability by defining topics in advance, while keeping an open mind towards differing views related to the topics (Flick, 2022). To achieve this, semi-structured interviews were conducted. The interview guide consisted of open questions, theory-driven questions, and confrontational questions.

Table 3-1: Overview of interviewees

Interviewee identifier	Position of interviewee	Company location	Industry	Company size (employees)	Group under study
I1	Legal director	USA	Software	500 - 1,000	Self-certified
I2	Senior consultant	France	Consulting	Up to 10	Self-certified
I3	Third-party software license manager	Germany	Multi-technology corporation	10,000+	Self-certified
I4	Senior manager OSS	Germany	Multi-technology corporation	10,000+	Self-certified
I5	Director third-party IT	United Kingdom	Software/ Semiconductors	5,000 – 10,000	Self-certified
I6	Assistant general counsel	USA	Hard- and software	10,000+	Self-certified
I7	Head of OSS competence center	Germany	Multi-technology corporation	10,000+	Self-certified
I8	OSS compliance manager	Japan	IT service provider	10,000+	Self-certified
I9	OSS compliance expert	India	Consulting	Up to 10	Self-certified
I10	OSS program office	Germany	Software	10,000+	Self-certified
I11	Software asset and license manager	Germany	IT service provider/Banking	1,000 – 5,000	Self-certified (in progress)
I12	OSS manager	South Korea	Software	1,000 – 5,000	Self-certified (in progress)
I13	Head of OSS	Germany	Software	5,000 – 10,000	Not certified
I14	Co-founder and CTO	United Kingdom	Software/ Healthcare	Up to 10	Third-party certified
I15	Director OSS services & IT sourcing	Germany	Consulting	10,000+	Third-party certification body
I16	Founder and CEO	Netherlands	Consulting	Up to 10	Third-party certification body
I17	CEO	United Kingdom	Consulting	Up to 10	Third-party certification body

Open questions are directed at the knowledge interviewees can provide immediately. The second type of questions results from the researcher's assumptions drawn from prior literature and serves to reveal the interviewees' implicit knowledge. Finally, confrontational questions give interviewees the chance to critically reassess their statements given so far, while taking into account competing alternatives (Flick, 2022). It started with general questions about the interviewee's company and position, followed by questions about the OSS compliance certification process itself, the motivation for the specific certification approach, and advantages and disadvantages of the certification.

In total, 17 interviews were conducted by me and two Master students from TUM School of Management between October 8, 2021 and July 6, 2022. The interviewees gave their consent to audio-record the conversation. All interviews were conducted virtually via Zoom or Microsoft Teams and lasted between 21 and 76 minutes, resulting in a total of 780 minutes of recording. Most interviews were conducted in English, some in German. For this study, quotes from interviews conducted in German were translated by me and are marked accordingly.

3.3.2 Data analysis

The recordings of the interviews were transcribed verbatim as preparation for the data analysis. Interpretation of the data followed the thematic coding approach suggested by Flick (2022). In this approach, a deep analysis of each single case results in a system of categories that is elaborated further by applying open coding and selective coding (comparable to Strauss (1987)). A cross-check of the constructed categories leads to a thematic structure which serves as basis for the analysis and comparison of further cases (Flick, 2022). Coding was performed with MAXQDA, a software for qualitative data and text analysis. To enhance the validity of the findings and to mitigate the presence of any research biases, I aimed for triangulation (Yin, 2009) by also letting two Master students at TUM School of Management perform the same coding approach with the data. Our outcomes matched well, underlining the credibility of the results.

3.4 Findings

3.4.1 Drivers for OSS compliance certification

Based on the interviews, several drivers for OSS compliance certification could be identified. They were grouped into external and internal drivers. Figure 3-2 represents an overview. The following subchapters explain the drivers in more detail.

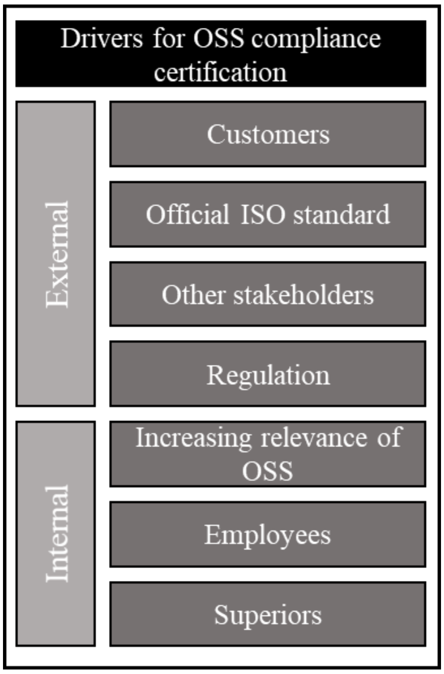


Figure 3-2: Drivers for OSS compliance certification

3.4.1.1 External drivers

The most important external driver for OSS compliance certification appears to be the customers. Although OSS compliance certification is nowhere near being part of every negotiation, there is a rising tendency of client firms asking for it (or at least specific aspects of the OSS compliance standard) (e.g., I14, October 20, 2021). Customers care for security issues that are closely entangled with OSS compliance. Especially the ability of suppliers to provide a SBOM, in which all third-party software components, including OSS, and the applicable licenses are listed, appears to be relevant (e.g., I5, November 16, 2021). Client firms demanding OSS compliance can even serve as an instrument for engaged employees to convince superiors of the need for certification, especially when "millions of dollars deals" are at stake (I5, November 16, 2021). Apparently, there are still huge industry differences when it comes to the relevance of the OSS compliance certification. One industry in which the positive trend is especially prominent is the automotive industry:

> "(…) It was a big automotive manufacturer. They themselves are not OpenChain certified, I believe. They demanded that all their suppliers, no matter which tier, were OpenChain certified. And this, of course, had some kind of viral effect that many, many companies which were suppliers [of this automotive manufacturer] aimed for the OpenChain certification."[9] (I11, November 3, 2021)

[9] Quote translated from German to English by the author.

The push from the customer side most probably will increase even further since the OSS compliance standard has become an official ISO standard (e.g., I4, October 27, 2021). Having a formal ISO standard helped to raise the awareness for OSS compliance significantly, as it is perceived as an "even more trustworthy, reliable instrument"[9] (I15, June 1, 2022). Due to the ISO standard, it is even expected that the OSS compliance certification will become part and parcel of the software procurement process as essential element of the purchasing conditions (e.g., I15, June 1, 2022).

Not only customers can serve as drivers for OSS compliance certification, but also other stakeholders. One example are suppliers that call their customers' attention to the topic and encourage them to seek certification themselves (I7, July 1, 2022). Moreover, engaged individuals, especially from the OpenChain community, spread the knowledge about the OSS compliance standard and thus serve as powerful drivers for the certification. They educate about the OpenChain Project and the certification on conferences and use every opportunity to raise awareness for OSS compliance (e.g., I5, November 16, 2021).

Finally, increasing regulation is expected to drive OSS compliance certification. One example is the "Executive Order 14028 on Improving the Nation's Cybersecurity"[10] issued by Joe Biden, the President of the United States of America, on May 12, 2021. It aims at improving cybersecurity through several initiatives with regard to the security and integrity of the software supply chain. One of the initiatives requires all suppliers that sell software and hardware to US agencies to be able to provide a SBOM, which is also one of the elements of the OSS compliance standard (I15, June 1, 2022). In general, the topic OSS compliance and thus the awareness for the related certification is more prominent in highly regulated industries with a large need for security, such as the automotive, defense, medical/pharmaceutical, chemical, or banking industry (e.g., I13, December 28, 2021).

3.4.1.2 Internal drivers

First and foremost, the increasing relevance of OSS for companies is a crucial internal driver to deal with the topic OSS compliance and ultimately to achieve OSS compliance certification. Most of the interviewees' companies were intensive OSS users, some of them were even aiming at using OSS in as many use cases as possible (e.g., I2, October 14, 2021). This does not only entail using OSS in daily work life, but also implementing OSS into own products and services (e.g., I5, November 16, 2021). Several companies

[10] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/, retrieved August 11, 2023

experienced a change of attitude towards OSS over the last years. They moved from seeing OSS as a threat towards embracing the huge potential of OSS (e.g., I6, October 31, 2021). Apart from using OSS, for several companies, contributing to OSS communities is also essential, including maintaining own OSS projects. Two companies even claimed to be "open by default" (I14, October 20, 2021). This was reflected, for example, in the decision to open source all code created inside the company. One firm even started as OSS project (I1, October 8, 2021). Due to the growing importance of OSS for companies, the topic OSS compliance is gaining relevance as well. All interviewees agreed that OSS compliance is essential, not only for the sake of risk management, but also to make sure "to play by the rules and maintain a healthy relationship with OSS communities" (I2, October 14, 2021).

In many companies, engaged individuals were the driving force for OSS compliance certification. Employees learned about the OpenChain Project and the certification either by stumbling over the homepage by coincidence, through their own engagement in the project, or through the exchange with peers and decide to drive the topic forward also in their own company (e.g., I11, November 3, 2021). They developed a personal ambition to achieve certification in their company and to show that their OSS compliance processes are best-in-class within their industry:

> "We were determined to prove that what we do is state-of-the-art. Nothing else. Just like a marathon runner who says: 'Now I want to finish in less than four hours.'"[9] (I7, July 1, 2022)

Finally, supportive superiors help to drive OSS compliance certification. They either support the ambitions of their employees or give themselves the order to achieve OSS compliance certification (e.g., I7, July 1, 2022).

3.4.2 Motives for OSS compliance certification

Figure 3-3 summarizes the identified motives for OSS compliance certification. Several motives relate to the certification itself; others are directed at a specific certification approach (self-certification or third-party certification). The following subchapters give more details about the different motives.

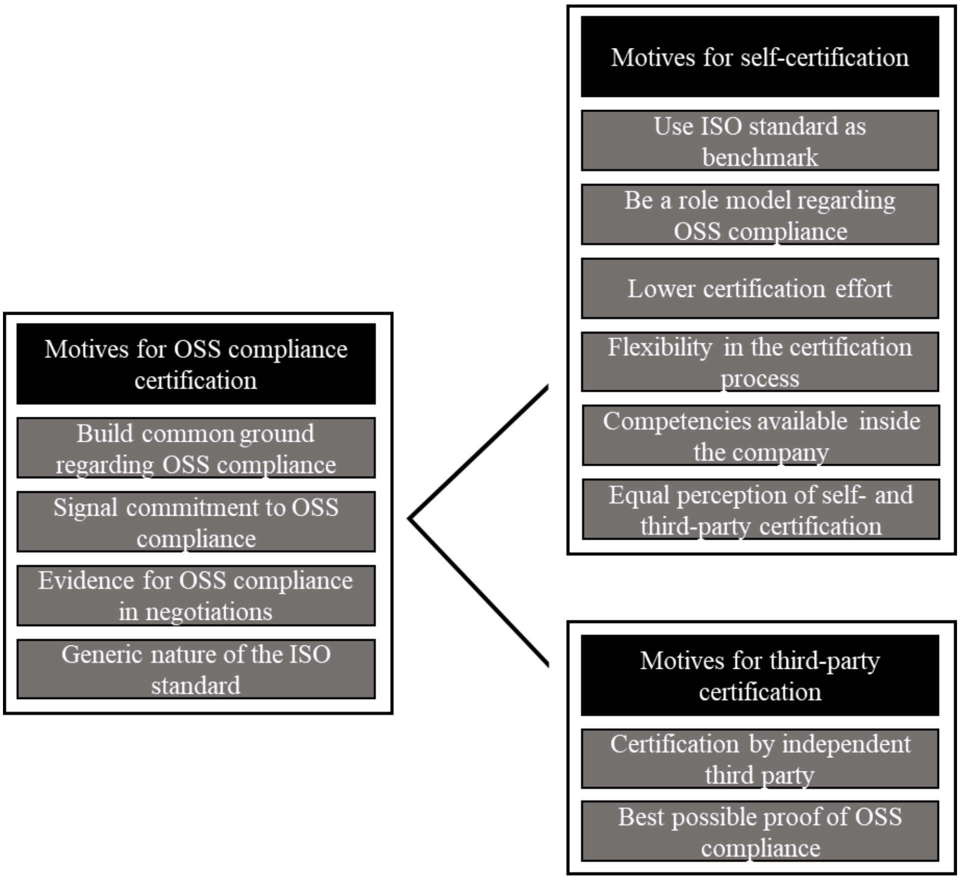

Motives for OSS compliance certification
Build common ground regarding OSS compliance
Signal commitment to OSS compliance
Evidence for OSS compliance in negotiations
Generic nature of the ISO standard
Motives for self-certification
Use ISO standard as benchmark
Be a role model regarding OSS compliance
Lower certification effort
Flexibility in the certification process
Competencies available inside the company
Equal perception of self- and third-party certification
Motives for third-party certification
Certification by independent third party
Best possible proof of OSS compliance

Figure 3-3: Motives for OSS compliance certification (general, self-, and third-party certification)

3.4.2.1 General motives

The most important motive for OSS compliance certification is to build a common ground regarding OSS compliance. The understanding of what OSS compliance is and what it comprises varies greatly. This becomes especially apparent in negotiations with customers and suppliers (e.g., I6, October 31, 2021). Every company has its own policies, processes, and delivery formats which makes it difficult to find a common ground in discussions. Hence, creating standards around OSS compliance is crucial (e.g., I13, December 28, 2021). In this context, OSS compliance certification serves as a huge facilitator:

> “The advantage is basically that if I talk to someone and I know [the company] is OpenChain certified, I have a starting point. Some sort of vocabulary that I can use. We don’t need to start with defining what is a distribution, what does a release mean. All of this is defined in this standard. So we have a common language. This is extremely important.“ (I7, July 1, 2022)

Related to building a common understanding of OSS compliance is creating awareness for the topic, not only among a company’s stakeholders but also internally. Having an official ISO standard for OSS compliance serves as catalyst in internal discussions to underline the importance of the topic and the risks related to insufficient

OSS compliance (e.g., I11, November 3, 2021). Consequently, OSS compliance certification can also help to increase trust in OSS. Many companies are still skeptical towards OSS, as they fear that "if anyone is contributing code, there is no quality [review] process" (I14, October 20, 2021). This uncertainty and doubt towards OSS mainly result from a lack of understanding. OSS compliance certification can help to mitigate this uncertainty (e.g., I6, October 31, 2021).

Another essential motive for OSS compliance certification is to signal commitment to OSS compliance internally and externally. Certification signals competence in OSS compliance, especially since the standard has become an official ISO standard (I5, November 16, 2021). Customers can be sure that a certified supplier follows rigorous processes, understands the obligations that come along with OSS licenses, and can provide a comprehensive list of OSS components implemented in their products. This leads to a higher level of transparency, credibility, and trust (e.g., I10, June 15, 2022). Consequently, certification can serve as a differentiating factor and help to stand out from competitors (I17, July 6, 2022). This effect can be enhanced by communicating the certification actively towards stakeholders (e.g., via press releases or presentations at conferences), although not many companies make use of this approach yet. The companies that chose active communication stressed certain aspects related to their certification, for example that they were the first to achieve certification in their industry or that they achieved it for the whole company and not only for certain business areas (e.g., I5, November 16, 2021). Yet, most companies only present their certification if stakeholders, especially customers, ask for it (e.g., I1, October 8, 2021). When it comes to internal communication, most companies announced the OSS compliance certification to their employees via their internal communication tools or at internal topic-related summits (e.g., I5, November 16, 2021).

In addition, certification serves as evidence for OSS compliance in negotiations and lawsuits. In the future, OSS compliance certification is expected to be sufficient proof for OSS compliance, reducing the negotiation effort significantly (I6, October 31, 2021). However, this status is by far not yet reached. Customers still tend to spend a large amount of time on reviewing OSS compliance-related quality control documents from suppliers (e.g., I11, November 3, 2021). Further, certification helps to increase confidence in the OSS compliance of targets in acquisition scenarios:

> "We know that across the ecosystem, there are varying degrees of OSS compliance. And we see it especially when we acquire companies that some companies are very good and some are an absolute mess. And so interestingly enough, if OpenChain conformance was important across

> the industry, it would probably help us just as much with our acquisitions as it would with actually just procuring software. (…) It will give us more confidence that they're doing it right. And will give us less mess to clean up." (I6, October 31, 2021)

OSS compliance certification can also be used as additional piece of evidence in case of a lawsuit to demonstrate compliance with regulatory obligations. It shows that a company adheres to the official ISO standard and has implemented all procedures claimed to be necessary to ensure OSS compliance. Yet, of course, being certified does not prevent being sued per se (e.g., I6, October 31, 2021).

Finally, the generic nature of the ISO standards motivates companies to achieve OSS compliance certification. It allows the application across all company sizes and industries, as it defines which measures need to be in place to be OSS compliant, rather than concrete ways how to implement them:

> "Imagine that you had a standard for bus driver safety training. So let's say I am operating a bus company in the middle of the desert in Africa and then you are operating a bus company in Northern Alaska. It would be silly for a standard to say you must know how to put snow chains on your bus. Because I don't need that in Africa in my desert, but I very much need it in Alaska. (…) Instead, [a standard] would say you need to describe the system you have in place for appropriate safety training given your anticipated conditions. (…) So you need to have it flexible enough to allow smart people to actually apply the appropriate requirements and training in this case for the situations that they're going to encounter and not for things they don't." (I6, October 31, 2021)

This example also illustrates that the standard setting organization by far cannot be aware of all industry- or even company-specific requirements. Thus, the decision about how to implement OSS compliance measures should lie with the experts themselves. An overly complex standard would not be adopted by companies (I2, October 14, 2021).

3.4.2.2 Motives for self-certification

Apart from general motives for OSS compliance certification, several motives specifically related to self-certification were identified. First and foremost, self-certification based on the ISO 5230 standard serves as a benchmark. Companies use the OSS compliance standard to cross-check already existing compliance processes to gain confidence that they are adequate and meet the most recent requirements (e.g., I8, December 28, 2021). Another aim is to confirm that engineers understand the existing OSS compliance processes and adhere to them (e.g., through an internal audit) (I5, November 16, 2021). If gaps in the compliance processes or a lack of adherence are discovered, usually a significant time investment is necessary to fix them. One company mentioned, for example, that they needed almost two years to convert their OSS compliance training into an online format to be able to meet the requirement of at least 85% of the workforce being trained regarding OSS compliance (I5, November 16, 2021). Another example was a company that used the ISO 5230 standard even for a complete redesign of existing compliance processes after having been acquired by other firms (I13, December 28, 2021). In further cases, the standard was used as benchmark to set up OSS compliance processes from scratch:

> "The whole topic OpenChain for me was simply a great blueprint or sort of a checklist. In the process creation, I could say ok, go through it, these are the things you definitely need to consider. And based on the minimum requirements from the OpenChain specification we could see how we position ourselves internally. So [finding the OpenChain Project] was really a lucky strike."[9] (I11, November 3, 2021)

The OpenChain Project provides an extensive amount of material to support companies in designing the processes. Moreover, the community is very supportive and provides personal guidance (I11, November 3, 2021).

For those companies that are active in the OpenChain Project and even co-developed the standard, it is especially important to be a role model for OSS compliance through self-certification. Following the motto "eat your own dog food", they are of the opinion that as co-creators of the standard they should also exemplify it (I7, July 1, 2022). They perceive themselves as multipliers for the OSS compliance standard and aim at spreading awareness for the topic.

Another relevant motive for self-certification is the lower certification effort. Compared to third-party certification, self-certification is commonly associated with a lower time and financial investment, as there is no need for commissioning an external certification body (e.g., I4, October 27, 2021). Hence, self-certification is also suitable for companies with insufficient resources. Related to the lower certification effort is the higher flexibility in the certification process. For self-certification, it is possible to flexibly choose the timeframe and the composition of the team involved in the process. In contrast, for the third-party certification process the certification body mostly dictates the timeframe and the team composition (e.g., I4, October 27, 2021).

Additionally, having the necessary competencies available inside the company is a motive and prerequisite for self-certification at the same time. As the company itself is responsible for cross-checking the conformity with the OSS compliance standard in this certification approach, it must possess the relevant competencies. According to many interviewees, they see the competencies necessary to assess OSS compliance rather with the companies than the certification bodies:

> “Am I ever going to get [third-party] certified? No. Why the heck would I? Because I know the topic better than any of the others since I've been there since the beginning. And I know a hell of a lot more than most auditors.” (I13, December 28, 2021)

The internal knowledge about company-specific demands regarding OSS compliance is more profound. Certifiers might know the ISO standard but are oftentimes not able to transfer its requirements to a specific product development process (I4, October 27, 2021).

Lastly, the rather equal perception of self- and third-party certification in the OSS compliance context speaks for the first-mentioned approach. The equal perception is driven by the fact that companies that wrongfully claim self-certification regarding OSS compliance face large reputational and ultimately financial damage in case of exposure (e.g., through negative publicity or lawsuits) (e.g., I5, November 16, 2021). Stakeholders, especially customers, always have the right to ask for proof of OSS compliance. Thus, cheaters would be uncovered as soon as details are requested, but cannot be delivered (e.g., I1, October 8, 2021). So far, most of the companies does not feel sufficient pressure to pursue third-party certification. As reliable enterprise partner, they have already established trust with their customers, which makes the need for formal certification obsolete (e.g., I6, October 31, 2021). Yet, if the return on investment is large enough (e.g., if large customers demand third-party certification), this stance might change. In general, the demand for third-party certification with respect to OSS compliance is expected to grow especially in highly regulated industries (I4, October 27, 2021). Another reason for the rather equal perception of self- and third-party certification is the large variety in expertise and credibility of the certifiers. So far, there is no official accreditation for certifiers yet when it comes to the ISO 5230 standard (e.g., from DAkkS, the national accreditation body of Germany) (I17, July 6, 2022). Some certifiers do not have an official accreditation as certification body at all (I15, June 1, 2022). Hence, prices and procedures related to the ISO 5230 certification vary greatly and companies cannot rely on an official proof of diligence yet when selecting a certifier.

3.4.2.3 Motives for third-party certification

When it comes to third-party certification, the main motive is to receive the confirmation of adequate OSS compliance measures from an independent third party. The unbiased view of the certification body and the external proof of OSS compliance is perceived as differentiator in pre-sales, especially when the certificate was issued by a renowned certifier (e.g., I15, June 1, 2022). This is the biggest difference to the self-certification approach, where there is always the option to “just click yes” in the online questionnaire and stakeholders need to rely on the honest self-assessment of companies (I14, October 20, 2021). Wrongful statements about OSS compliance in the self-certification process might happen “out of malice, a lack of honesty and management, or maybe as well a lack of competence” (I15, June 1, 2022). Further, for third-party certification, recertification is obligatory after a certain time (partial reassessment after one year, full reassessment after three years). Thus, it requires a certain long-term commitment from companies. If companies are not willing to undergo recertification, the certificate can be withdrawn again (I15, June 1, 2022). The final advantage of third-party certification are possible liability claims companies have against the certification body. The issuing organization to some extent bears liability for damages that are directly related to the certification outcome (I15, June 1, 2022).

In summary, third-party certification is the best possible proof of OSS compliance. It provides evidence for “internal process and management excellence”[9] and attests companies to be “best-in-class”[9] (I15, June 1, 2022). It serves, for example, as highest official proof in lawsuits or towards stakeholders that the board members have taken sufficient measures regarding OSS compliance to avert possible risks from a company (according to §93 AktG):

> “If in lawsuits the question appears whether the management has implemented adequate [OSS compliance] measures (…) related to this risk and you can say: ‘I don’t have anything here, I don’t consider open source at all.’ Then this is bad. If you can say: ‘Well, I am OpenChain self-certified and I think we have it under control.’ Then this is already better. Yet, ideally you would be able to say: ‘We are officially externally audited and certified.’ There is nothing more you can do. If something happens now, we have fulfilled our duty.”[9] (I15, June 1, 2022)

3.4.3 Deterrents to OSS compliance certification

Besides motives for OSS compliance certification, the interviews also revealed several deterrents. Figure 3-4 provides a summary.

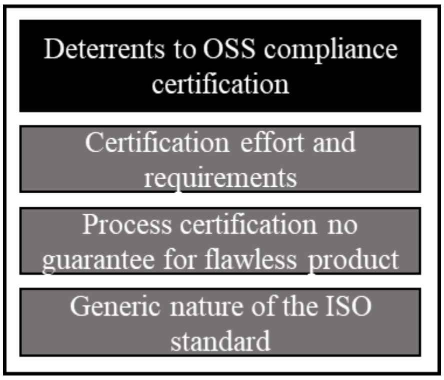

Deterrents to OSS compliance certification
Certification effort and requirements
Process certification no guarantee for flawless product
Generic nature of the ISO standard

Figure 3-4: Deterrents to OSS compliance certification

First, the certification effort and requirements prevent companies from seeking OSS compliance certification. Especially small companies do not have the capacity to fulfill all standard requirements. Usually, they do not have the manpower to cover all roles and responsibilities regarding OSS compliance (I3, October 15, 2021). Yet, a clear definition and assignment of roles and responsibilities is a prerequisite of the standard. For example, the appointment of a contact person internal and external stakeholders can approach in case of questions regarding OSS compliance is obligatory (I2, October 14, 2021). Companies need to make sure that the responsible employees have sufficient time to fulfill the respective roles or even need to hire new staff to take over the related tasks. Hence, the certification effort might outweigh the advantages for companies, especially when they still feel isolated regarding OSS compliance and do not see any benefit for the software supply chain (I2, October 14, 2021). Besides the certification effort, companies might not agree with certain requirements of the standard. One interviewee criticized the obligatory training of employees regarding OSS compliance:

> “(…) I don’t give training to my engineers on open source. And so here is where OpenChain and we differ. (…) So OpenChain requires us to train all developers once a year. We decided not to. (…) You might ask why the heck are you not doing this? Very simple. Most of these trainings are going in to one ear and going out the other ear. (…) They don’t give the developers the tools that are actually applicable to their work, (…) It’s completely utterly useless for most developers.” (I13, December 28, 2021)

Another example are the requirements regarding the format in which documents need to be provided. The standard requires the written form, whereas some companies might prefer different formats. One firm, for example, provides their OSS policy as code. Their reasoning is that developers would not read a policy consisting of dozens of pages anyway. Instead, they provide a computable policy which engineers can directly use to scan their projects and find possible flaws (I13, December 28, 2021). Approaching topics differently than required by the standard thus might lead to the decision not to strive for OSS compliance certification.

A further reason that speaks against OSS compliance certification is the fact that process certification is no guarantee for flawless products. It may still well happen that a product contains flaws regarding OSS compliance, although it went through the certified processes. The main reason is that processes usually involve people and people make mistakes (e.g., I4, October 27, 2021).

> „So OpenChain might help ensure that the processes you have in place make sense and are good, but it doesn't mean you're actually conforming. It's possible that I have a process that

> misses things. And in fact, I can guarantee if anyone tells you they're not missing anything, they're either lying to you or they don't understand how this works.” (I6, October 31, 2021)

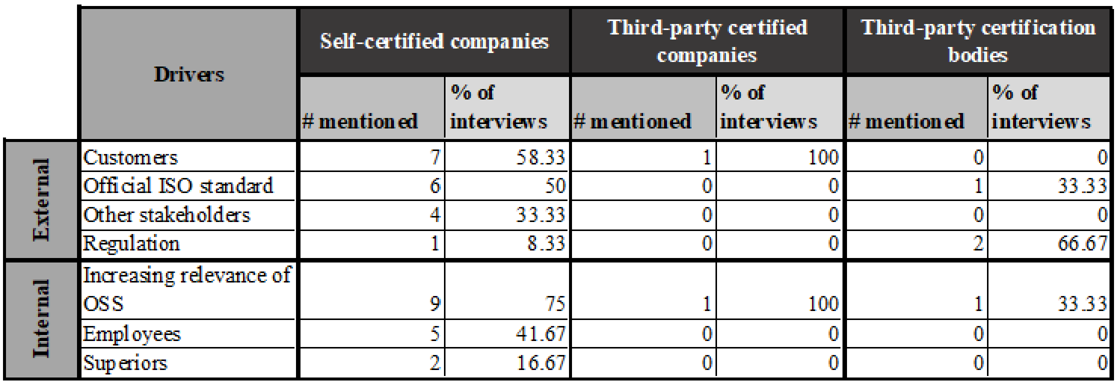
Thus, OSS compliance certification should focus on assessing “operating effectiveness”, rather than solely “design effectiveness”. This means that it should not only be considered how processes are set up and documented, but also how they are put into practice in the daily business. Processes might appear plausible on paper, but employees do not implement them properly (I15, June 1, 2022).

Finally, the generic nature of the ISO standard is not only perceived as motive for OSS compliance certification, but also as deterrent. As the standard is formulated rather generally and does not define how certain measures need to be implemented, companies struggle to translate it into working processes (e.g., I13, December 28, 2021). Following the standard might even add an administrative burden and complexity to a firm (I17, July 6, 2022). Moreover, the generic nature creates a certain leeway for companies and certifiers with respect to the thresholds they set to consider requirements of the standard as fulfilled. Some companies or certifiers might accept a manually created SBOM, others require a tool-generated one (I15, June 1, 2022). This adds to the large diversity of processes falling under the certification, making it difficult for stakeholders to assess its rigor.

3.5 Discussion

This study sheds light on the factors that drive or hinder companies to achieve OSS compliance certification. Looking at potential external drivers, customers appear to be the most relevant one for self-certified and third-party certified companies. They were mentioned in 58.33% of the interviews in the first group and in 100% of the second group (see Table 3-2). Certification bodies consider regulation as most relevant driver (mentioned in 66.67% of the interviews). The fact that the OSS compliance standard has recently been recognized as official ISO standard is another relevant factor for self-certified companies (appears in 50% of the interviews). From an internal perspective, the increasing relevance of OSS for companies is the most decisive driver for all three groups. 41.67% of the self-certified companies also consider the commitment of individual employees as significant.

Table 3-2: Relevance of drivers for OSS compliance certification across groups



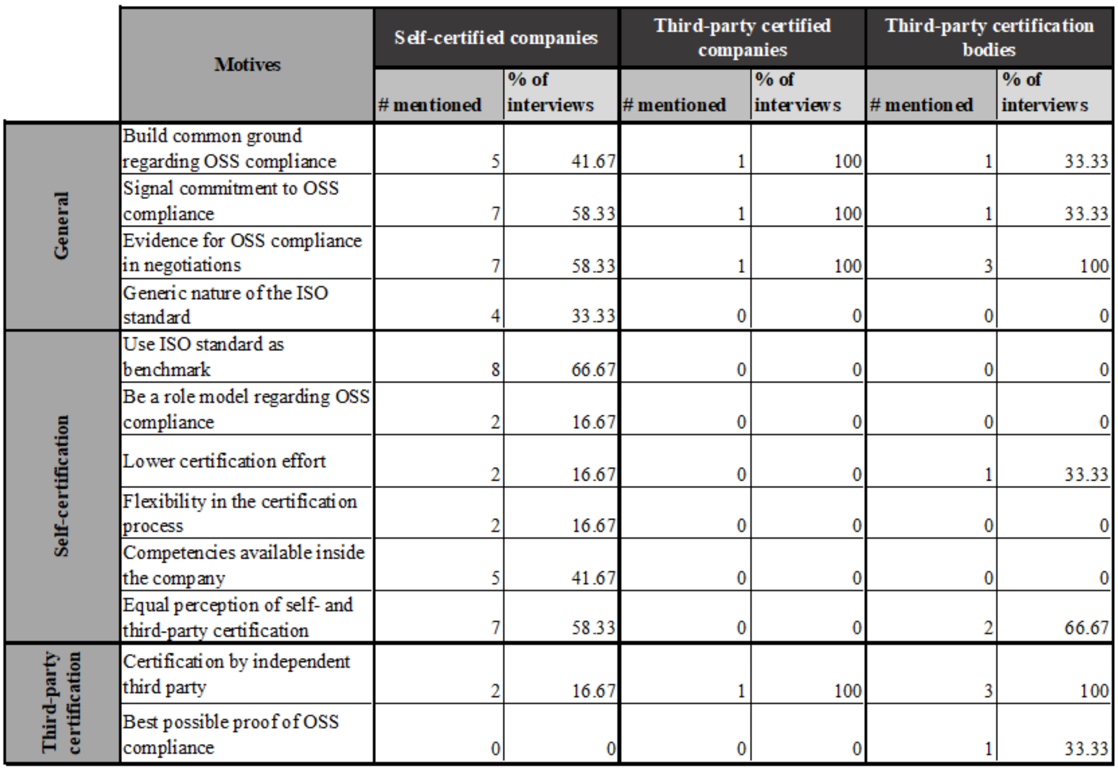
	Drivers	Self-certified companies		Third-party certified companies		Third-party certification bodies	
		# mentioned	% of interviews	# mentioned	% of interviews	# mentioned	% of interviews
External	Customers	7	58.33	1	100	0	0
	Official ISO standard	6	50	0	0	1	33.33
	Other stakeholders	4	33.33	0	0	0	0
	Regulation	1	8.33	0	0	2	66.67
Internal	Increasing relevance of OSS	9	75	1	100	1	33.33
	Employees	5	41.67	0	0	0	0
	Superiors	2	16.67	0	0	0	0

Regarding general motives for OSS compliance certification, the ability to use it as evidence for OSS compliance in negotiations is the most decisive factor across all three groups (see Table 3-3). Self- and third-party certified companies thereby stress negotiations with customers, whereas certification bodies emphasize negotiations in the acquisition context. For self-certified companies, signaling commitment to OSS compliance is an equally important motive for seeking certification (mentioned in 58.33% of the interviews), followed by building a common ground regarding OSS compliance (41.67%). These two general motives are also relevant for third-party certified companies and certification bodies.

When it comes to specific motives for self-certification, the most prominent one mentioned by 66.67% of the self-certified companies is to use the ISO standard as benchmark, mostly to cross-check existing OSS compliance processes, but also to set up processes from scratch. The fact that self- and third-party certification are perceived equally so far also speaks for the self-certification approach (appears in 58.33% of the interviews). Two-thirds of the interviewed certification bodies also support this perception. Finally, 41.67% of the self-certified companies consider having the necessary competencies available inside the company as further motive for self-certification.

The most relevant motive for third-party certification across all three groups is the involvement of an independent third party that impartially assesses OSS compliance. All interviewed third-party certified companies and certification bodies mentioned this motive. Even 16.67% of the self-certified companies mentioned this factor as advantage of third-party certification. 33.33% of the certifiers consider third-party certification the best possible proof of OSS compliance for companies.

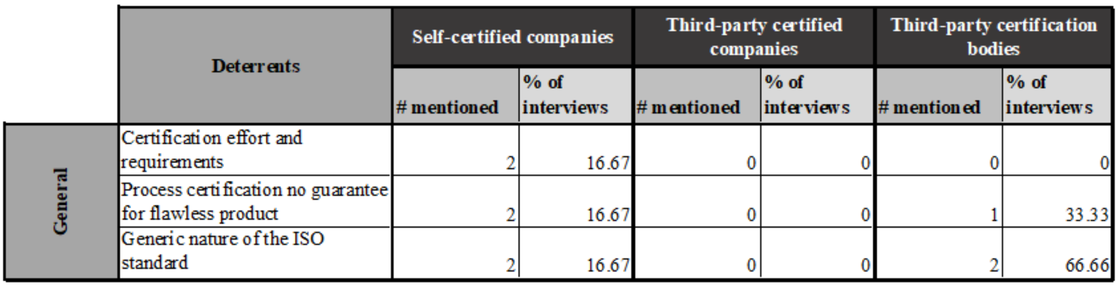
Table 3-3: Relevance of motives for OSS compliance certification across groups



	Motives	Self-certified companies		Third-party certified companies		Third-party certification bodies	
		# mentioned	% of interviews	# mentioned	% of interviews	# mentioned	% of interviews
General	Build common ground regarding OSS compliance	5	41.67	1	100	1	33.33
	Signal commitment to OSS compliance	7	58.33	1	100	1	33.33
	Evidence for OSS compliance in negotiations	7	58.33	1	100	3	100
	Generic nature of the ISO standard	4	33.33	0	0	0	0
Self-certification	Use ISO standard as benchmark	8	66.67	0	0	0	0
	Be a role model regarding OSS compliance	2	16.67	0	0	0	0
	Lower certification effort	2	16.67	0	0	1	33.33
	Flexibility in the certification process	2	16.67	0	0	0	0
	Competencies available inside the company	5	41.67	0	0	0	0
	Equal perception of self- and third-party certification	7	58.33	0	0	2	66.67
Third-party certification	Certification by independent third party	2	16.67	1	100	3	100
	Best possible proof of OSS compliance	0	0	0	0	1	33.33

Lastly, this study also reveals several deterrents to OSS compliance certification. The generic nature of the ISO standard is not only perceived as advantage, but also as downside. 66.66% of the certification bodies and 16.67% of the self-certified companies criticized that due to the general formulation, firms struggle to translate the standard into working processes and certifiers lack guidance regarding which processes to consider as certifiable (see Table 3-4). These two groups also agree that a process certification does not guarantee flawless products. Finally, 16.67% of the interviewed self-certified companies are of the opinion that the certification effort and its requirements prevent firms from seeking OSS compliance certification.

Table 3-4: Relevance of deterrents to OSS compliance certification across groups



	Deterrents	Self-certified companies		Third-party certified companies		Third-party certification bodies	
		# mentioned	% of interviews	# mentioned	% of interviews	# mentioned	% of interviews
General	Certification effort and requirements	2	16.67	0	0	0	0
	Process certification no guarantee for flawless product	2	16.67	0	0	1	33.33
	Generic nature of the ISO standard	2	16.67	0	0	2	66.66

3.6 Implications for theory and practice

With this study, I contribute to the literature on ISO certification (Anderson et al., 1999; T. Y. Lee, 1998; Quirós & Justino, 2013) by adding several factors to the motives and deterrents researchers already identified. While I could confirm the relevance of most of the external certification drivers (e.g., customers, regulation), I was able to add significant insights on internal factors. In the case of ISO 5230 certification, the commitment of individual employees and the increasing relevance of the topic OSS compliance for companies push firms towards seeking certification. Moreover, I add the new perspective of distinguishing between self-certification and third-party certification. Most relevant motives for self-certification appear to be the usage of the ISO standard as benchmark to cross-check existing processes or design new ones, the equal perception of self- and third-party certification, as well as the availability of the necessary competencies inside the company to achieve certification. In contrast, the assessment of OSS compliance measures by an independent third party is the most important factor that speaks for third-party certification. Another important insight from this study is the ambiguous perception of the generic nature of ISO standards. On the one hand, it allows the application in varying industries and across different company sizes according to the specific company requirements. On the other hand, it does not provide companies with sufficient guidance on how to set up adequate processes, sometimes resulting in processes that do not work in practice. Further, certifiers face a significant leeway with respect to the thresholds they set to consider requirements of the standard as fulfilled. Hence, some certification bodies might certify certain processes that others regard as insufficient. Of course, this circumstance is quite specific to the ISO 5230 standard, as it was introduced only recently and no official accreditation for certifiers is available yet.

From a practical perspective, this study also provides several implications. For companies that think about seeking certification according to a certain ISO standard, it provides insights into potential advantages and downsides. So far, to my best knowledge, ISO 5230 is the only standard for which the two different approaches (self- and third-party certification) exist. Yet, the study might support companies in their decision whether to strive for the one approach or the other. Through this study, organizations maintaining ISO standards gain knowledge about what motivates companies to achieve ISO certification and what hinders them. In addition, they should take into account the ambiguous perception of the generic nature of most ISO standards and provide companies with further material to enable them to translate the standards into processes that fulfill the standard requirements and fit to the company environment.

3.7 Limitations and avenues for future research

The results of this study are based on the 17 conducted interviews. While I could reach twelve companies that are self-certified or are currently in the self-certification process, I was only able to speak to one representative from a single third-party certified company, which makes it difficult to gain comprehensive insights for this group. Identification of third-party certified companies was difficult, as all ISO 5230 conformant firms are mentioned together on the OpenChain website, regardless of the certification approach. Moreover, the interviewed certification bodies were not able or not allowed to provide information on companies that they certified as a third party. Thus, gathering additional data from third-party certified firms would lead to a more balanced picture of the results and increase their generalizability. The same is valid for certifiers, although for this group, I was already able to speak to three of the eleven organizations that currently offer third-party certification regarding OSS compliance.

Further, when interpreting the results, it should be taken into account that the majority of the interviewees in the group of self-certified companies were highly involved in the OpenChain Project and thus very committed to the topic OSS compliance. Some of them were even founding members and supported the development of the standard and the self-certification approach. Therefore, it is very likely that these interviewees per se have a more positive attitude towards OSS compliance certification in general and more specifically, towards self-certification. Companies that have a more skeptical view on this approach or have undergone non-diligent self-certification are probably not willing to participate in an interview (or are at least not willing to admit it).

Finally, as the ISO 5230 standard has only been introduced by the end of 2020 and thus is not yet well-established, future research should examine the drivers and motives for certification several years later to find out whether they change over time. Especially when it comes to the perception of self- and third-party certification, a significant difference is expected in the future. With the standard becoming more popular across different industries, the demand for third-party certification from stakeholders (e.g., customers) will probably increase, especially in highly regulated industries.

4 The role of open source software compliance certification in the software supply chain – Insights from a conjoint experiment[11]

4.1 Introduction

In the software supply chain, the role of OSS is increasing steadily and with it the topic OSS compliance (see chapter 3.2.1) (Morgan et al., 2013). Companies that do not fulfill the OSS license obligations face a significant risk of lawsuits against them, ultimately leading to substantial financial and reputational losses. Hence, the awareness of the necessity to adequately manage OSS compliance is growing constantly. Not only do companies increasingly care for their own OSS compliance, but also expect it from their suppliers. The topic is gaining relevance in supplier negotiations with customers asking for specific OSS compliance elements (e.g., SBOM). However, there is not yet a common understanding across industries of what OSS compliance means and which measures need to be in place. Thus, managing OSS compliance when acquiring software with OSS components from external suppliers is especially challenging.

Many companies have realized this issue and developed the OSS compliance standard (ISO/IEC 5230) to facilitate OSS compliance (see chapter 3.2.2). Based on this standard, companies can achieve a self-certification or third-party certification (The Linux Foundation, 2022). The aim of the standard is to create a common understanding of OSS compliance and create a software supply chain in which OSS is procured with consistent compliance information. The corresponding certification should support software suppliers in credibly signaling their OSS compliance to their customers and other stakeholders.

My study investigates the question of how this certification is perceived by firms when selecting software suppliers. I investigate the importance of certification as a criterion in the decision to select a software supplier and distinguish between no certification, self-certification, and third-party certification. Answering this question provides valuable insights into the role of OSS compliance certification in the software supply chain and helps software suppliers to decide whether it might be worth pursuing such certification. Moreover, it contributes to our theoretical understanding of the integration of OSS in commercial activities of companies.

[11] This chapter is based on a paper co-authored by Michael A. Zaggl and Jörn Block. It has been submitted to the European Journal of Information Systems.

I build on signaling theory to theorize how OSS compliance certification can help to overcome information asymmetries between the supplier and acquirer of software. Taking on the signal receiver’s perspective (i.e., the perspective of the company that wants to acquire software), I formulate hypotheses on the role of a software supplier’s OSS compliance certification relative to other selection criteria known to be effective signals for supplier quality (i.e., previous collaboration with the software supplier, supplier’s experience in the respective areas, supplier’s received recommendations from its customers, and total cost of ownership of the software). I also hypothesize different perceptions of self-certification vs third-party certification as well as moderating factors that might explain potential differences in perception.

Empirically, this study builds on a discrete choice-based conjoint experiment (Louviere & Woodworth, 1983), in which real-world software purchasing experts were asked to choose between offers from different software suppliers that all contain OSS components. The design of the conjoint experiment, specifically the selection of the decision criteria, was based on interviews with experts regularly involved in the selection of software suppliers.

My results show that OSS compliance certification is a decision-relevant criterion for selecting a software supplier. Its relative importance in the sourcing decision is comparable to first-hand experience with suppliers through previous collaboration. A comparison of self- with third-party certification shows that software suppliers with third-party certification are chosen about 2.5 times more likely than self-certified suppliers. Awareness of the regulatory standard ISO 5230 and the perceived risk of OSS procurement are critical moderating factors. Being aware of the ISO 5230 standard significantly increases the positive effect of self-certification, resulting in a reduced gap between the two forms of certification. The perceived risk of OSS procurement increases the positive effect of third-party certification. It has, however, no influence on the effect of self-certification.

My findings offer relevant implications for theory. First and foremost, I identify OSS compliance certification as a new and relevant phenomenon in the entanglement of OSS and companies. The literature on OSS certification is so far focused on certifying OSS itself, reflecting a strong product-focus (Feuser & Peleska, 2010; Kakarontzas et al., 2010). The approach examined in this study aims at certifying underlying OSS compliance processes instead. Hence, I add a new perspective to this literature stream. In IS research, the effect of software certifications has been investigated in the B2C sector (Kaplan & Nieschwietz, 2003; Nöteberg et al., 2003). The study examines the concept of compliance certification in the software supply chain and thus transfers the issue of certification to the B2B sector, more specifically to the OSS context. Second, beyond my main contribution to the literature on company-involved OSS development, I also contribute to the signaling and certification literature (Connelly et al., 2011; Kalliamvakou et al., 2016; Lins & Sunyaev, 2017). I add ISO 5230 awareness and perceived risk of OSS procurement as boundary conditions of signal receivers that influence how receivers interpret certain signals. Moreover, to the best of my knowledge, I am the first to distinguish between self-certification and third-party certification in this literature stream.

The results also have relevant implications for practitioners. For software suppliers, one relevant implication is that certification for OSS compliance is an important signal they should provide to their potential customers. Organizations that maintain standards can significantly increase the credibility of rather uncommon certification approaches such as self-certification by spreading the knowledge about certain standards and the different certification approaches. Hence, software suppliers may consider not spending large amounts of money on third-party certification and focusing on a thorough self-certification instead.

4.2 Background

4.2.1 OSS certification

OSS certification is a recent development in the literature (Kalliamvakou et al., 2016). One main research area in this literature compares the certification of OSS with proprietary software, highlighting differences among stakeholder groups and in the development and testing process (Fabbrini et al., 2013; Fusani & Marchetti, 2010; Morasca et al., 2009). A major insight is that for OSS, a product-focused certification appears to be more suitable than a process-focused certification due to the less closely monitored development process and the unrestricted accessibility of the source code (Feuser & Peleska, 2010; Kakarontzas et al., 2010). Due to the openness of OSS, research suggests a certification approach based on peer reviewing, but also acknowledges that it would be challenging to manage such a community-driven certification process (Feuser & Peleska, 2010). As a first step, it had been suggested to become part of the education of software engineering trainees to raise awareness for this certification approach (Khoroshilov, 2009).

Another research area deals with the economic challenges related to OSS certification. The certification of safety critical software is costly and requires several steps. After the certification, changes in the system are usually not allowed anymore to avoid recertification. This approach is not suitable for OSS, as it is subject to regular changes. Thus, researchers suggest a continuous certification approach, making systems certifiable at any point in time (Comar et al., 2009). Further, researchers introduced different OSS development approaches that support the aim of producing certifiable and reusable OSS (e.g., OPEN-SME) (Kakarontzas et al., 2010).

Finally, research focuses on the certification of OSS safety and security. The security certification approach typically applied for closed source solutions is mostly based on a checklist. This approach is not suitable for OSS security certification. Several researchers showed this by detecting security vulnerabilities in OSS that traditional certification programs could not find (Helms & Williams, 2011; King et al., 2012; Smith et al., 2010). One way to overcome this issue would be to improve existing test scripts by including implementation level vulnerabilities.

All these findings underline the clear product orientation in OSS certification. The OSS compliance certification approach investigated in this study displays a strong process orientation instead, adding a new perspective to this literature stream. Rather than certifying OSS itself, the procedure aims at certifying company processes to secure compliance with the obligations that go along with OSS licenses.

4.2.2 Signaling theory

This study builds on signaling theory (Connelly et al., 2011; Spence, 1973). More concretely, it builds on literature about signals that convey information about unobservable supplier quality (Biong, 2013; Kirmani & Rao, 2000). Figure 4-1 illustrates the signaling timeline.

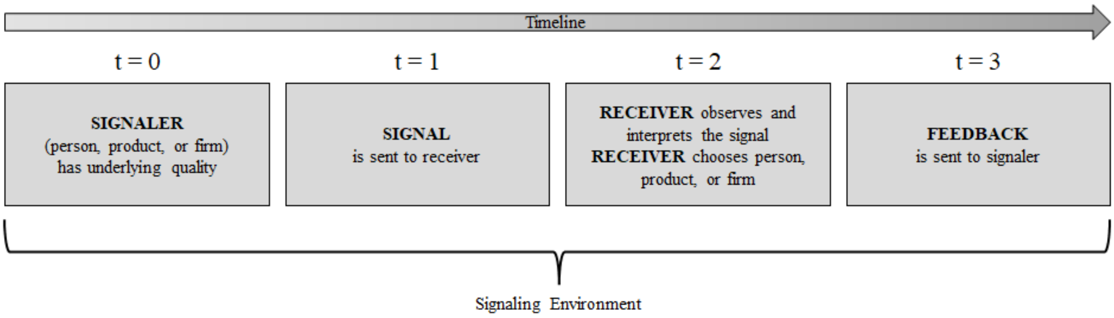


Figure 4-1: Signaling timeline (based on Connelly et al. (2011))

Signaling theory focuses on reducing information asymmetries that occur between two parties by initiating measures to convey positive, unobservable qualities of a signal sender (Spence, 2002). Such information asymmetries also exist between a buying company and a software supplier. When selecting a supplier, the company cannot fully judge the capabilities and quality of the different providers of software. In other words, the suppliers possess certain information about their quality that is not available for potential customers, but that could be useful for them. Thus, it might be beneficial for the suppliers to transmit various signals to communicate this information. The potential customers receive the signals, give meaning to them, and draw conclusions. In case of successful signaling, the supplier as signal sender benefits through the resulting actions from the buying company (i.e., being selected as software supplier). Hence, the signaling theory is adequate to explain how OSS compliance certification can help to overcome information asymmetry regarding OSS compliance between the software supplier and acquirer compared to other proven quality signals.

Main elements of the signaling theory are the two involved parties (i.e., the signal sender and the signal receiver), the signal itself, and the signal environment (i.e., institutional environment, competitive environment) (Connelly et al., 2011; Lins & Sunyaev, 2017). For a signal to be effective, it has to fulfill certain requirements. First, it has to be observable. This criterion is related to the extent to which signal receivers are able to become aware of the signal (Connelly et al., 2011). Second, it has to be costly. Signals are normally associated with significant costs for the signaler, making it difficult to imitate the signal. If the sender cannot provide the quality transmitted by the signal, it probably leads to a significant reputation loss, resulting in a potential loss of future profits (Connelly et al., 2011; Riley, 2001). Taking this into account, the signal receiver rationally should consider signals about the sender's unobservable quality to be credible because false claims would result in financially unattractive outcomes (Rao & Monroe, 1996; Tirole, 1988). Based on this fact, researchers have added a signal category which is not associated with a significant up-front investment, but rather with the risk of losing future profits (i.e., nondissipative signals) (Bhattacharya, 1980; Rao et al., 1999).

4.3 Hypothesis development

4.3.1 Software supplier's certification for OSS compliance

According to the International Organization for Standardization (1996), certification is defined as "written assurance that a product, process, or service conforms to specified requirements”. This definition fits the third-party certification approach available for the ISO 5230 standard. An independent certification body (e.g., TÜV Süd AG, PricewaterhouseCoopers GmbH) checks a company’s conformity with the requirements of a sound OSS compliance program determined in ISO 5230. In case of a positive assessment, a written confirmation is issued. The third-party certification comes along with high costs for the company; not only in monetary terms, but also regarding time investment, as several own employees are usually involved to support the certification process.

Prior literature acknowledges such third-party certifications as reliable signals. They are observable and involve a significant up-front investment. Yet, empirical findings about certification effectiveness are not conclusive (Lins & Sunyaev, 2017). When looking at the IT sector, several studies, mostly in the B2C sector, have found a positive effect on the customer’s willingness to purchase (Kaplan & Nieschwietz, 2003; Nöteberg et al., 2003). In contrast, various studies exist that have not found any significant effect (Hui et al., 2007; Mauldin & Arunachalam, 2002). In a study by Lang et al. (2018) on decisive factors for the selection of cloud service providers, certification reached rank 8 out of 13 identified relevant criteria.

Literature on supplier selection in the B2B sector (irrespective of software or not) draws a clearer picture. A study by Biong (2013) found a positive effect of a corporate social responsibility certification on the tendency to select a supplier’s offer. In addition, Goebel et al. (2018) found that purchasing managers are willing to pay a 2.59% price premium if the supplier can ensure compliance with certain sustainability standards via external accreditation rather than only signing a respective contract (i.e., minimum level of assurance). My study draws on these results, leading to the following hypothesis:

H1a: A software supplier’s certification for OSS compliance (self-certification or third-party certification) has a positive effect on the likelihood of the supplier being selected.

In contrast to third-party certification, self-certification appears to be an easier and less costly way to show conformity with the key requirements of a sound OSS compliance program. Based on the ISO 5230 standard, the OpenChain Project offers a free online questionnaire covering all relevant elements. After completing the questionnaire and uploading certain verification material, the company receives a badge confirming that all essential criteria are met. Companies can display this badge on their homepage or use it in the communication with stakeholders. They also can announce their conformity with the ISO 5230 standard on the OpenChain homepage (The Linux Foundation, 2022). Thus, the criterion of signal observability is met. Yet, at first glance, self-certification does not involve a significant upfront investment and thus does not fulfill the second traditional characteristic of a signal (i.e., signal cost). Instead, it is associated with the risk of losing future profits, which is in line with the definition of a nondissipative signal. Hence, self-certification is expected to be a weaker signal compared to third-party certification, resulting in the following hypothesis:

H1b: The effect of self-certification for OSS compliance on being selected is weaker than the effect of third-party certification on being selected.

My interviews with OpenChain representatives and companies which underwent self-certification revealed that the self-certification process means a significant investment. If done thoroughly, several employees from different departments are involved in the process for weeks or even months. Based on the reference material provided by the OpenChain Project, existing OSS compliance processes in the company need to be questioned and adapted if necessary. If one or several essential criteria of the ISO 5230 standard are not met, new processes or policies have to be established. Hence, a thorough self-certification does not only mean ticking the boxes in an online questionnaire but scrutinizing existing processes and in many cases process adaptation. Companies that are aware of the ISO 5230 standard and the intended self-certification procedure might be able to better assess the investment associated with a thorough OSS compliance self-certification process, increasing its credibility and signal effectiveness.

These insights lead to the assumption that being aware of the ISO 5230 standard increases the positive effect of self-certification on the likelihood of a software supplier being selected. I pose a similar assumption for the effect of third-party certification. My two hypotheses are as follows:

H2a: The positive effect of self-certification for OSS compliance on the likelihood of a software supplier being selected is stronger if the decision maker is aware of the ISO 5230 standard.

H2b: The positive effect of third-party certification for OSS compliance on the likelihood of a software supplier being selected is stronger if the decision maker is aware of the ISO 5230 standard.

In organizational buying decisions, the importance of perceptions of a supplier increases with the perceived risk of a purchase (Johnston & Lewin, 1996; Wu & Gaytán, 2013). With growing risk associated with a sourcing situation, factors like product and service quality become of utmost importance. Purchasing experts will conduct extensive active information search using various information sources. In later stages of the purchasing process, personal, non-commercial sources (e.g., external consultants) tend to be favored (Johnston & Lewin, 1996). Further, in purchase situations associated with high risk, formal decision rules are rather prominent. All these measures serve to support managing the perceived risk related to a purchase by creating a sense of credibility through in-depth evaluation (Blombäck & Axelsson, 2007). These results indicate that the positive perception of third-party certifications might be largely driven by the level of risk the buying party associates with the purchase. This assumption is strengthened by research in the B2C sector. Angulo and Gil (2007) found that consumers' perception of beef safety is negatively related to the likelihood of paying a price premium for certified beef. In addition, Brach et al. (2018) identified perceived risk of sustainable products as a mediating variable that positively influences consumers' purchase intentions toward certified sustainable products compared to those without certification.

Translating these insights to the context of purchasing software containing OSS components, it has to be taken into account that buyers may vary in their risk perception of OSS procurement. The risks associated with OSS which were mentioned most frequently in the survey part of this study were that not complying with OSS licenses leads to a significant reputational (64.76% approval) and financial loss (54.29%). Further, the concern of OSS adoption making the business unit highly dependent from the respective OSS community or the software supplier was mentioned by almost half of the respondents (47.62%). Purchasing experts who attribute high risk to OSS procurement might value a third-party certification for OSS compliance higher compared to those with a lower perceived risk. For self-certification, by contrast, a negative influence of perceived risk of OSS procurement is expected. In this certification approach, the independent third party is missing which would take care of a neutral assessment and thus reduces the risk associated with the purchasing scenario. Hence, I derive the following two hypotheses:

H3a: The positive effect of self-certification for OSS compliance on the likelihood of a software supplier being selected is weaker if the decision maker perceives the risk of OSS procurement to be high.

H3b: The positive effect of third-party certification for OSS compliance on the likelihood of a software supplier being selected is stronger if a decision maker perceives the risk of OSS procurement to be high.

Figure 4-2 provides an overview of the hypotheses and the resulting research model.

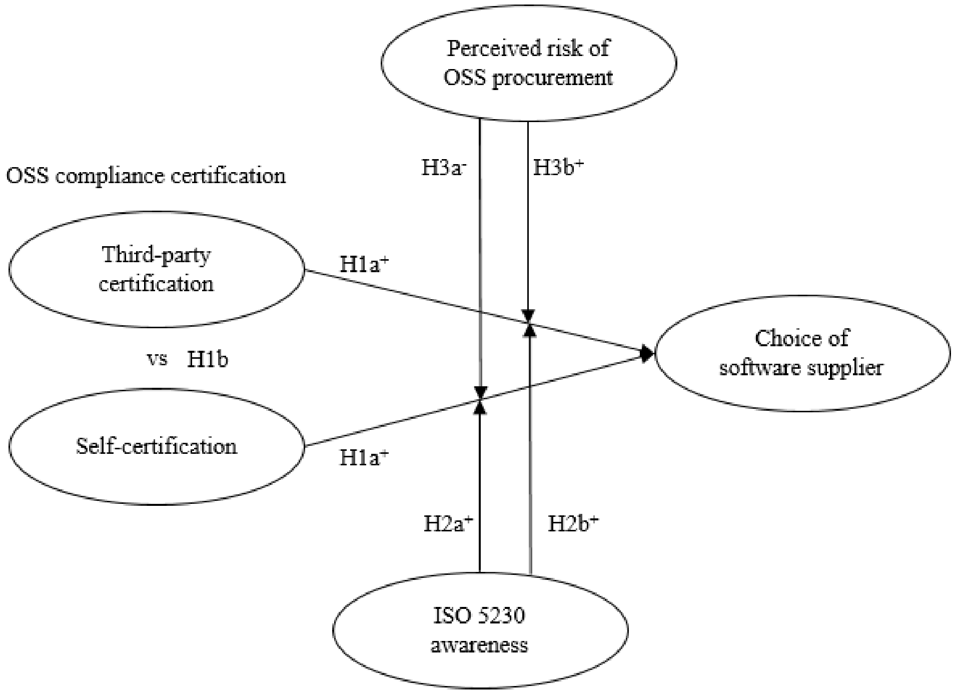

Perceived risk of OSS procurement
OSS compliance certification
H3a-
H3b+
Third-party certification
H1a+
Choice of software supplier
vs H1b
Self-certification
H1a+
H2a+
H2b+
ISO 5230 awareness

Figure 4-2: Research model

4.3.2 Further criteria and quality signals in (software) sourcing decisions

To conduct a choice-based conjoint experiment, I need to choose further decision criteria besides OSS compliance certification. As literature applying signaling theory in the software context is scarce, I primarily draw on the supplier choice literature from other contexts in which signaling plays a central role to identify decision-relevant attributes for my design.

Software supplier's relevant experience

Companies care about whether a supplier exhibits knowledge in relevant areas of expertise and has realized similar projects before. Michell and Fitzgerald (1997) found that IT suppliers who have a track record in the relevant areas are more likely to be chosen. According to Spence (1974), from an individual perspective, signals can be reflected in human capital itself. Examples are individual characteristics such as education or job experience (Spence, 1974). Transferring this perception to an organizational perspective, company experience can serve as a signal that can picture the quality of the sender and makes customers perceive the sender as credible (R. Helm & Mark, 2007; Kaas, 1991). A study by Ho and Wei (2016) that adopts the signaling theory in the IT outsourcing context revealed that past experiences of IT outsourcing service suppliers positively influenced perceived service quality.

Previous collaboration with a software supplier

When publishing a call for tender, companies usually receive offers from already known, but also unfamiliar suppliers. Michell and Fitzgerald (1997) found that most of the information technology (IT) supplier selection processes for new contracts are indeed open, meaning that both known and unknown suppliers have equal chances to be chosen. In contrast, when enhancing or renewing existing contracts, IT suppliers who delivered a satisfying performance in prior collaborations have a considerable advantage (Michell & Fitzgerald, 1997). However, we know from other contexts in which signaling plays a central role that this advantage appears to exist also for new contracts. In the manufacturing or market research sector, for example, positive impressions gained through the delivery of high-quality products or smooth interactions with key employees of the supplier in former joint projects are factors that companies consider relevant in the selection process (Blombäck & Axelsson, 2007; Wuyts et al., 2009). A good supplier-customer relationship built in earlier collaborations increases the likelihood of the supplier being chosen in a subsequent procurement decision (Biong, 2013; Blombäck & Axelsson, 2007). The investment in high-quality products and services in former collaborations and the resulting reputation thereby promise high quality also in future periods (Blombäck & Axelsson, 2007; Shapiro, 1982).

Recommendations from a software supplier's customers

We learn from research adopting signaling theory in other B2B contexts that recommendations from other customers can be a meaningful signal of quality, especially when companies cannot rely on their own experiences with the supplier (Boyd et al., 2022; S. Helm & Salminen, 2010; Kotler & Pfoertsch, 2007; Wuyts et al., 2009). References from other customers, especially renowned ones, are central for suppliers in the process of creating a credible company brand name (S. Helm & Salminen, 2010; Salminen & Möller, 2006). In B2B markets, brands stand for high-quality performance and lead to a higher perceived value among customers. Thereby, they help to reduce complexity in supplier selection decisions (Kotler & Pfoertsch, 2007).

Total cost of ownership of the software

When selecting IT suppliers, research has found that cost is not decisive, as long as it does not lie outside the acceptable range (Michell & Fitzgerald, 1997). In other contexts, however, cost is an important factor. Wathne et al. (2001) showed, for example, that corporate customers are likely to switch to another commercial bank for cost reasons. Even strong interpersonal ties with the former bank cannot avoid this (Wathne et al., 2001). Biong (2013) also found a negative relationship between a high price offered and the likelihood of subcontractors being chosen. These findings are based on the (somewhat counterintuitive) assumption that a low price can serve as a signal for high quality. According to Kirmani and Rao (2000, p. 69), a low launch price represents a "sale-contingent, default-independent" signal. In particular, high-quality suppliers might use a low price to encourage customers to try out their offering for the first time. If the product or service is of high quality, the chance for repeat purchases increases. Thus, high-quality suppliers voluntarily forego current profits for a long-term customer relationship with future receipts (Kirmani & Rao, 2000). Yet, there also exists a contrary perspective on the effect of cost on buying decisions. Companies might be willing to pay more in return for receiving high quality, as a low price may be associated with low quality and thus makes customers suspicious (Michell & Fitzgerald, 1997; Monroe & Dodds, 1988).

Based on the interviews with software purchasing experts that I conducted prior to my experiment, it became clear that in their context, total cost of ownership is the decisive criterion rather than solely the purchasing price. In sourcing situations, the experts take into account the overall cost of the software project throughout its life cycle (i.e., cost of acquiring, using, managing, and withdrawing). Hence, I chose total cost of ownership rather than purchasing price as a decision criterion in this experiment.

4.4 Method

4.4.1 Research design

To shed light on the decision-making of experts involved in software sourcing, to understand the relative importance of OSS compliance certification compared to other signals in the supplier selection process, and to identify possible trade-offs, I conducted a choice-based conjoint experiment (Louviere & Woodworth, 1983). This method was first applied in the marketing area to examine the relative importance of product features (e.g., Green & Srinivasan (1990)). Since then, it has been used in several studies in the area of supplier selection (Biong, 2013; Wathne et al., 2001; Wuyts et al., 2009).

Compared to post hoc methods (e.g., interviews, surveys), conjoint experiments present certain advantages when investigating decision behavior. Post hoc methods rely on information from the past and thus might have to bear recall and rationalization biases (Zacharakis & Meyer, 2000). In contrast, conjoint experiments collect real-time information while decisions are made. Therefore, this method mimics the actual behavior of decision makers more accurately. Every decision for or against a software supplier requires making trade-offs between the supplier criteria. This fact can be mapped appropriately within a conjoint experiment.

I applied a discrete choice-based conjoint experiment. This means that the participants had to choose between two hypothetical offers from software suppliers that vary in several attributes. Moreover, I added a no-choice option, so that participants could also decide not to choose any of the two offers. I chose a choice-based rather than a rating-based conjoint design, as it is more realistic and better reflects the real-life decision scenario. After having evaluated proposals from several potential supplier candidates and having conducted extensive rounds of negotiations, experts typically have to decide between the offers from the last two remaining suppliers (or choose no supplier at all). The attributes were chosen based on a qualitative pre-study (i.e., interviews with experienced experts regularly involved in the selection of software suppliers, companies with ISO 5230 certification, and representatives of the OpenChain Project) and a literature review (see section 4.3), following the procedure suggested by Wathne et al. (2001). Each conjoint attribute has three levels (see Table 4-1).

The overall conditions of the initial situation and the decision scenario were explained to the participants on the introductory page to align their viewpoints. Participants were asked to think about a typical software sourcing situation for their business unit[12] with regard to total cost of ownership and sourcing purpose (i.e., use in the company or implementation into own products) of the software project. After having conducted negotiations with several possible suppliers, two suppliers are left. Both suppliers have offers that contain OSS components. Both offers are identical regarding technology fit, time-to-market, and contract law (including service and warranty agreements). Yet, they might differ in the attributes explained above. When moving the mouse over the attributes, more detailed descriptions appeared to ensure a common understanding among participants (see descriptions in Table 4-1).

[12] The term “business unit” thereby refers to the entity in the company which the participant can make the most concrete statements about (e.g., team, business unit, entire company).

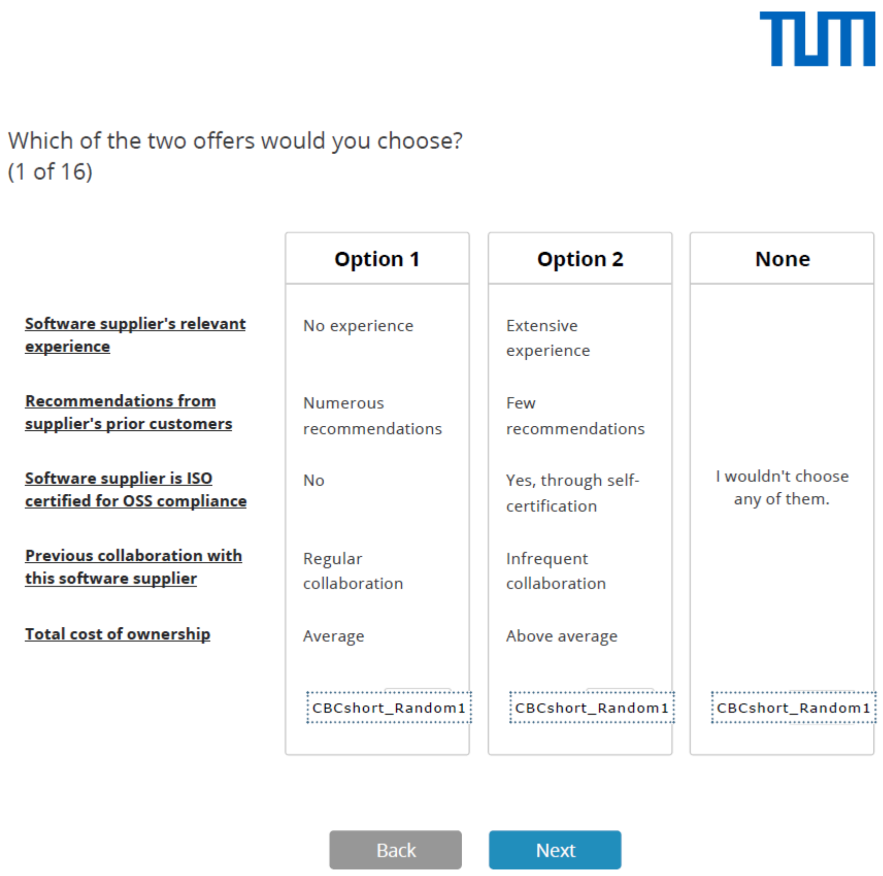
Table 4-1: Overview of attributes and attribute levels

Attributes	Description of attributes	Levels
Software supplier's relevant experience	The supplier and its key personnel are familiar from past joint projects.	- No experience - Little experience - Extensive experience
Previous collaboration with a software supplier	The supplier has realized similar projects before.	- No collaboration - Infrequent collaboration - Regular collaboration
Recommendations from software supplier's prior customers	Other customers recommend this supplier based on their prior collaboration experience.	- No recommendations - Few recommendations - Numerous recommendations
Software supplier is ISO certified for OSS compliance	Aim of OSS compliance measures: Ensure to meet license requirements and minimize risks when using and implementing OSS. ISO 5230 certification attests measures to ensure compliance with OSS requirements (e.g., written OSS policy, process to create bill of materials, etc.); achievable through free self-certification (online questionnaire plus providing documentation) or by a third party.	- No - Yes, through self-certification - Yes, through a third party
Total cost of ownership of the offered software	Overall cost of the software project throughout its life cycle (including cost of acquiring, using, managing, and withdrawing)	- Below average - Average - Above average

I applied a full-profile choice-based conjoint design in which all previously mentioned attributes are included to make sure that the decision makers get a holistic impression of the hypothetical offers. Based on the attributes and the respective levels, 200 experimental designs were created. Each design represented a unique choice task consisting of two hypothetical software offers with different combinations of attribute levels. To not overwhelm the participants with too many choice tasks, I decided for a reduced conjoint design (Chrzan & Orme, 2000). Every participant faced 16 decision scenarios. 13 of them were randomly assigned and 3 scenarios were held constant across all participants. These fixed tasks ("hold-out tasks") help to estimate the test-retest-reliability of the participants' decisions.

Choice-based conjoint experiments can suffer from various order effects (Chrzan, 1994). To avoid these effects, I took three measures. First, to counterbalance potential biases caused through the order of choice tasks, they were randomly ordered within each of the 200 experimental designs. Further, to prevent negative order of options effects, also the two software offers were randomly ordered within each choice task. Finally, the order in which the attributes appeared was randomized across participants but was held equal for each respondent. By doing so, it can be avoided that the attribute which always appears first is subconsciously valued higher than the later ones. The whole study was pre-tested by a software sourcing expert and several colleagues to ensure the face validity of the design. The test participants checked whether the conjoint tasks were understandable, plausible, and not overly complex. Figure 4-3 illustrates an exemplary choice task.

The conjoint experiment is followed by a questionnaire. This part was primarily designed to shed light on business units' attitude towards OSS and OSS compliance and their familiarity with the OpenChain Project and the ISO 5230 standard. Finally, questions about the respondents' position and personal background, the business unit itself, and the respective company were posed.



Which of the two offers would you choose?
(1 of 16)

	Option 1	Option 2	None
Software supplier's relevant experience	No experience	Extensive experience	I wouldn't choose any of them.
Recommendations from supplier's prior customers	Numerous recommendations	Few recommendations	
Software supplier is ISO certified for OSS compliance	No	Yes, through self-certification	
Previous collaboration with this software supplier	Regular collaboration	Infrequent collaboration	
Total cost of ownership	Average	Above average	
	CBCshort_Random1	CBCshort_Random1	CBCshort_Random1

Figure 4-3: Exemplary choice task

I opted for a multilevel (hierarchical) logistic regression because the data consists of two levels (i.e., several decision observations for each respondent). Hence, the levels are not independent from each other. A multi-level approach allows to evaluate effects on cross-level interactions while the decisions are intricate (Aguinis et al., 2013). The individual decisions (choose the offer: "yes" or "no") reflected the binary dependent variable. The attribute levels serve as independent variables. Thus, the following regression equation results:

$$\log\left(\frac{\varphi_{ij}}{1-\varphi_{ij}}\right) = \beta_{0j} + \beta_{ij}x_{ij}$$

$$\text{with } \beta_{ij} = \gamma_{i0} + u_{ij}$$

φ_{ij} stands for the probability of a positive decision conditional on β_j for the choice *i* of respondent *j*. The independent variables *x* for the choice *i* of respondent *j* are reflected by x_{ij}. The independent variables are the attribute levels; for each attribute, one attribute level was used as reference level.

4.4.2 Measurement of the constructs "ISO 5230 awareness" and "perceived risk of OSS procurement"

To capture "ISO 5230 awareness", the survey part of the study contained a question on whether the respondents were aware of the ISO 5230 standard, the International Standard for OSS license compliance. The answer options were "Yes" and "No". The distribution was well balanced with 53.33% of the participants being aware of the ISO 5230 standard and 46.67% being not aware.

"Perceived risk of OSS procurement" was captured by taking the average value of three items measured on a 5-point Likert scale (1 = "completely disagree" to 5 = "completely agree"). The items were "OSS procurement is associated with a high level of risk", "There is a high level of risk that the expected benefits of procuring OSS will not materialize", and "Overall, I consider the procurement of OSS in my business unit to be risky". The items were adopted from Benlian and Hess (2011) who use them to measure the perceived risk of adopting software-as-a-service applications and were adapted to the OSS procurement context (Benlian & Hess, 2011; Featherman & Pavlou, 2003). Cronbach's alpha was 0.83, indicating a decent reliability (Cronbach, 1951).

4.4.3 Sampling and data collection

Participants in the study were experts involved in the selection of software suppliers. Main sources to identify suitable participants were mailing lists covering the target group (e.g., OpenChain Project, ToDo Group, OSB Alliance, Bitkom Working Group Open Source) and a manual search via LinkedIn. The search focused on experts with positions in relevant areas, using the keywords "software procurement/sourcing/purchasing" (plus respective translations into German), "software asset management", and "software category manager". The response rate for the participants acquired through LinkedIn was 11.5% (637 people contacted; 73 participants). The response rate for mailing lists was 1.9% (1,493 mailing list members; 29 participants). Three further participants were informed by colleagues about the study. In total, 105 respondents completed the questionnaire.

The conjoint experiment and the questionnaire were set up with Lighthouse Studio. The link to the study was shared with the potential participants together with a short description of the aim of the research project. After one and two weeks, respectively, reminders were sent out. Participants were offered access to the study results after answering all questions. Moreover, for every completed questionnaire five euros were donated to a non-profit organization.

4.4.4 Examination of potential biases in the data collection

4.4.4.1 Decision-making patterns and duration per choice task

Analyzing decision-making patterns and the duration per choice task (i.e., time statistics measure) gives insights into the quality of the responses and thus helps to assess whether respondents took the participation in the experiment seriously or whether the choice task was too trivial.[13] In web-based surveys there is the risk of participants clicking through without carefully reading the questions. One way to uncover this "clicking-through" behavior is to check whether the time to answer a choice task lies significantly below the average time per choice task reported in other studies that applied choice-based conjoint experiments. Another indicator for this behavior is when a respondent's choice pattern does not show any variation (i.e., always selecting the same alternative in the decision scenarios).

Figure 4-4 illustrates that the median response time per choice task successively decreases from 43 to 12 seconds. Prior research has found that participants only need about one third of the time to complete later choice tasks compared to the first one (Johnson & Orme, 1996). This behavior is largely reflected in this study as well. The average time spent to complete a choice task was 46 seconds. This appeared quite high, which is why I took a closer look at the averages for each participant. It became apparent that one participant spent 25,235 seconds (about seven hours) for one single choice task. I assume that this participant left the questionnaire open for such a long time and completed the questionnaire later. When I calculated the average time spent to complete a choice task without considering this participant, the result was 29 seconds, which is in line with prior studies (Johnson & Orme, 1996). Taking these analyses into account, one

[13] https://sawtoothsoftware.com/resources/knowledge-base/design-and-methodology-issues/how-to-use-time-statistics-to-improve-your-results, retrieved June 29, 2023

participant apparently displayed "clicking-through" behavior. This participant always selected the first option in the choice tasks and the time spent on each choice task lay clearly below the average duration reported in comparable studies. Hence, this participant was excluded from the final sample.

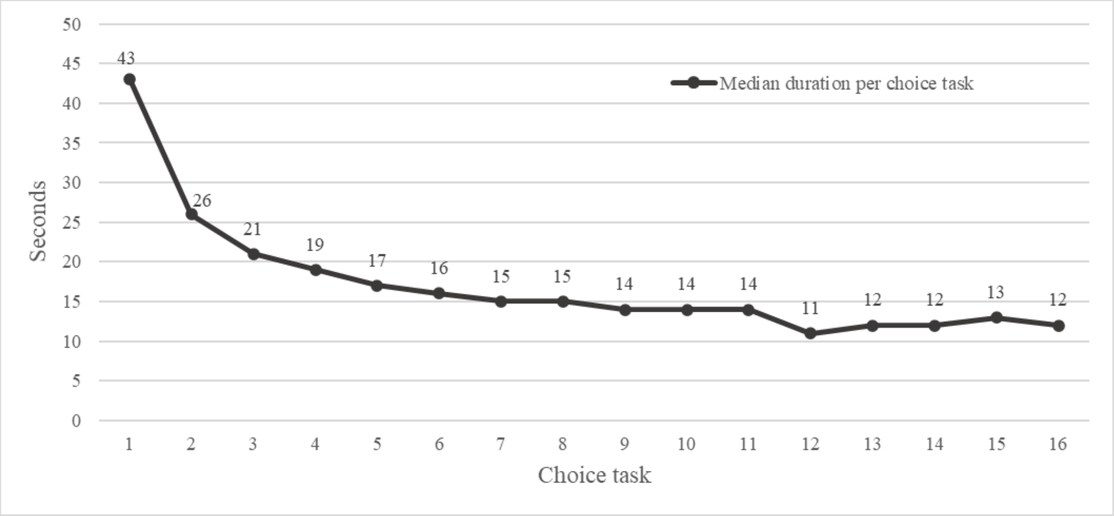
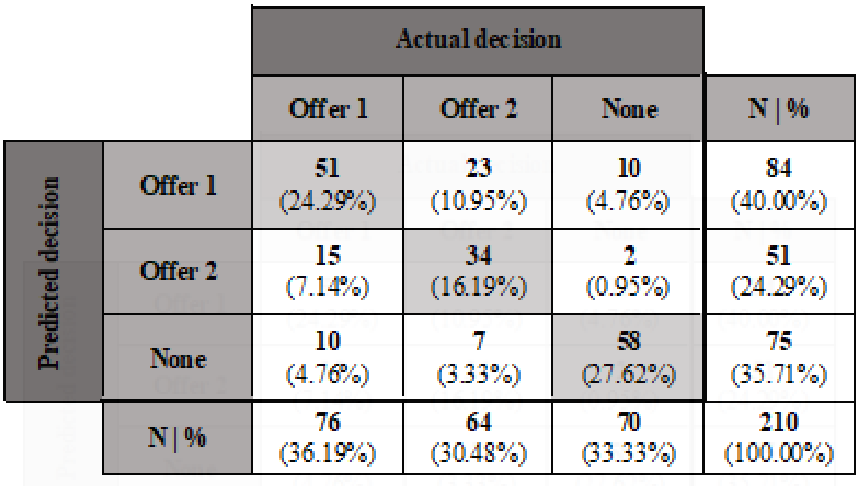


Figure 4-4: Median response time per choice task

4.4.4.2 Test-retest reliability

Another relevant question is whether the conjoint experiment reflects a suitable predictor for real decision scenarios (i.e., reliability) and thus attests the study a certain validity. However, actual validity can hardly be tested. Instead, I focus on estimating a proxy for the test-retest reliability of the participants' decisions. This is achieved by analyzing how well the 13 random choice tasks are able to predict the outcome for the two hold-out tasks (two of the three hold-out tasks were identical; only the two different ones are considered). It is a common approach to test predictive ability and to assess conjoint validity (Chrzan, 2015). I use a Hierarchical Bayes model (Lenk et al., 1996) to calculate the utility estimates for the 13 random choice tasks. Then I entered the utility estimates into the market simulator of Lighthouse Studio (provided by Sawtooth Software), a tool to conduct conjoint studies, to predict the choices for the two hold-out tasks for the 105 participants. The outcome is depicted in the confusion matrix in Table 4-2. For this study, the test results in an accuracy of 68.1% (24.29% + 16.19% + 27.62%) for the prediction of hold-out task choices with the support of the estimated utilities from the random choice tasks. This value is comparable to prior studies. For his study, for example, Shepherd (1999) found a test-retest reliability of 69%.

Table 4-2: Test-retest reliability via hold-out tasks



		Actual decision			
		Offer 1	Offer 2	None	N | %
Predicted decision	Offer 1	51 (24.29%)	23 (10.95%)	10 (4.76%)	84 (40.00%)
	Offer 2	15 (7.14%)	34 (16.19%)	2 (0.95%)	51 (24.29%)
	None	10 (4.76%)	7 (3.33%)	58 (27.62%)	75 (35.71%)
	N | %	76 (36.19%)	64 (30.48%)	70 (33.33%)	210 (100.00%)

4.5 Results

4.5.1 Overview of the sample

35.2% of the respondents' business units belonged to the information and communication technology industry, followed by 18.1% from manufacturing/logistics and 13.3% from engineering. 67.6% of the participants were located in Germany, 12.4% in other European countries, 6.7% each in Asia and the USA, and 1.0% each in South America and Africa. 19.0% of the companies had less than 250 employees. 48.6% of the respondents' companies employed over 10,000 people. 12.4% of the participants stated that their company has annual gross revenues of under $1 million, whereas 49.5% mentioned revenues of over $1 billion. 11.4% of the respondents' companies were younger than 10 years and 61.9% were older than 30 years.

24.8% of the participants held manager positions, 14.3% were department heads, and 14.3% were technical specialists. Main tasks of the participants included legal issues (mean = 3.68; 5-point Likert scale), procurement (mean = 3.50), and product development activities (mean = 3.10). The experience with software procurement reached a mean value of 3.79 on a 5-point Likert scale. No respondent thereby stated to have "no experience" with software procurement. This result indicates that the participants belonged to the target group of my study.

4.5.2 Results on the importance of decision criteria

Model 1 in Table 4-3 represents the results of the main model. The log-odds coefficients represent the importance that decision makers assign to each attribute level.

Table 4-3: Main regression model and models with interaction effects

Regression type: multi-level logistic regression with random intercepts and random slopes			
		Decision Log-odds	
Attributes and levels	Model (1)	Model (2)	Model (3)
Experience: extensive	2.604***	2.613***	2.609***
	(0.234)	(0.236)	(0.236)
Experience: little	1.057***	1.064***	1.059***
	(0.146)	(0.146)	(0.146)
(reference: no experience)			
Collaboration: regular	1.403***	1.403***	1.408***
	(0.155)	(0.155)	(0.157)
Collaboration: infrequent	0.596***	0.588***	0.602***
	(0.140)	(0.141)	(0.140)
(reference: no collaboration)			
Recommendations: numerous	0.877***	0.874***	0.889***
	(0.138)	(0.138)	(0.139)
Recommendations: few	0.336*	0.335*	0.341*
	(0.148)	(0.147)	(0.149)
(reference: no recommendations)			
Certification: third-party [H1a; H1b]	1.272***	1.125***	0.228
	(0.165)	(0.230)	(0.514)
Certification: self [H1a; H1b]	0.903***	0.590**	0.727
	(0.145)	(0.192)	(0.406)
(reference: no certification)			
TCO: above average	-0.797***	-0.798***	-0.793***
	(0.174)	(0.172)	(0.174)
TCO: average	-0.107	-0.105	-0.108
	(0.121)	(0.121)	(0.122)
(reference: below average TCO)			
dummy_ISOawareness		-0.682*	
		(0.286)	
ISOawareness X Certification: third-party [H2b]		0.303	
		(0.343)	
ISOawareness X Certification: self [H2a]		0.615*	
		(0.289)	
OSSprocurerisk			-0.425*
			(0.172)
OSSprocurerisk X Certification: third-party [H3b]			0.415*
			(0.211)
OSSprocurerisk X Certification: self [H3a]			0.0714
			(0.176)
Constant	-3.476***	-3.129***	-2.413***

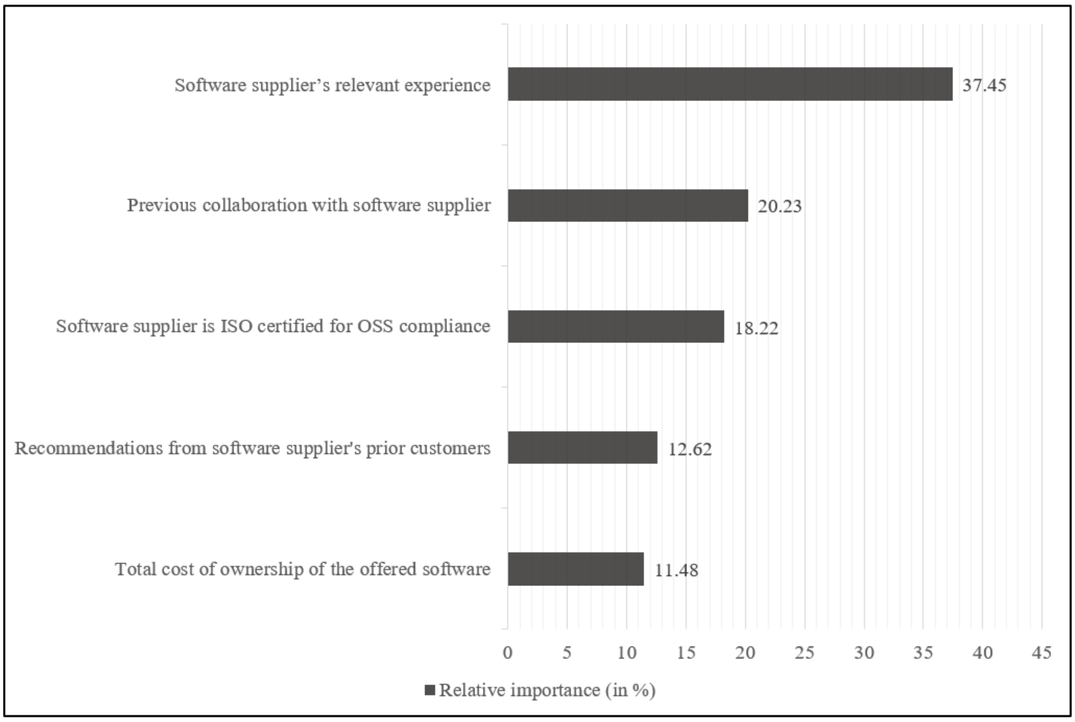
	(0.283)	(0.283)	(0.409)
var(_cons[sys_respnum])	0.590**	0.566**	0.558**
	(0.200)	(0.186)	(0.185)
Wald test		9.41*	10.42*
N (decisions)	2,730	2,730	2,730
N (decision makers)	105	105	105

Robust standard errors in parentheses; *** p<0.001, ** p<0.01, * p<0.05; TCO = Total Cost of Ownership

I also tested a multinomial logistic regression model, which allowed us to include the no-choice option in addition to the two choices presented in each scenario. This model shows a negative utility of the no-choice option as opposed to choosing one of the two alternatives (no-choice constant = -0.20). This outcome indicates that a sufficient number of combinations exist that are perceived better than the no-choice option.

To enable a more intuitive comparison of the attributes and their perceived importance, I estimated the relative importance of each attribute based on the regression results. Therefore, I divided each attribute's part-worth utility range by the sum of all attributes' part-worth utility ranges. The values were normalized (i.e., the sum of all relative importance values equals 100). Figure 4-5 shows the relative importance values for all attributes. The higher the value is for an attribute, the higher is its impact on the supplier selection decision of a decision maker.

The results show that the software supplier's experience is the most important attribute. It accounts for 37.45% of the total utility of a decision maker involved in selecting software suppliers. This attribute is approximately three times as relevant as recommendations from prior customers of the supplier (12.62%). Thus, recommendations from prior customers of the supplier play a comparably minor role in the decision. Previous collaboration and software supplier's ISO certification for OSS compliance appear to be rather important decision attributes (20.23% and 18.22%). Together, the three most important factors explain over 75% of the decisions. Hence, the likelihood of a software supplier being chosen increases if a supplier reflects high levels in these three attributes. In contrast, customers do not seem to put much importance on total cost of ownership when selecting software suppliers (11.48%). When looking at the levels of this attribute more closely, only total cost of ownership above average has a significant negative effect on the decision. On the other hand, decision makers seem to be indifferent between average and below average total cost of ownership.



Notes: Calculated based on the coefficients of the main model (Table 4-2). Reading example: With a relative importance of 37.45%, decision makers consider a software supplier's relevant experience about three times as important as the total cost of ownership of the offered software (11.48%). A software supplier's relevant experience accounts for 37.45% of the decision makers' total utility.

Figure 4-5: Relative importance of attributes

Finally, I calculated the odds ratios of each attribute level based on the coefficients of the main model (Model 1 in Table 4-3) to get an even more detailed picture of the effect sizes. Figure 4-6 displays the results.

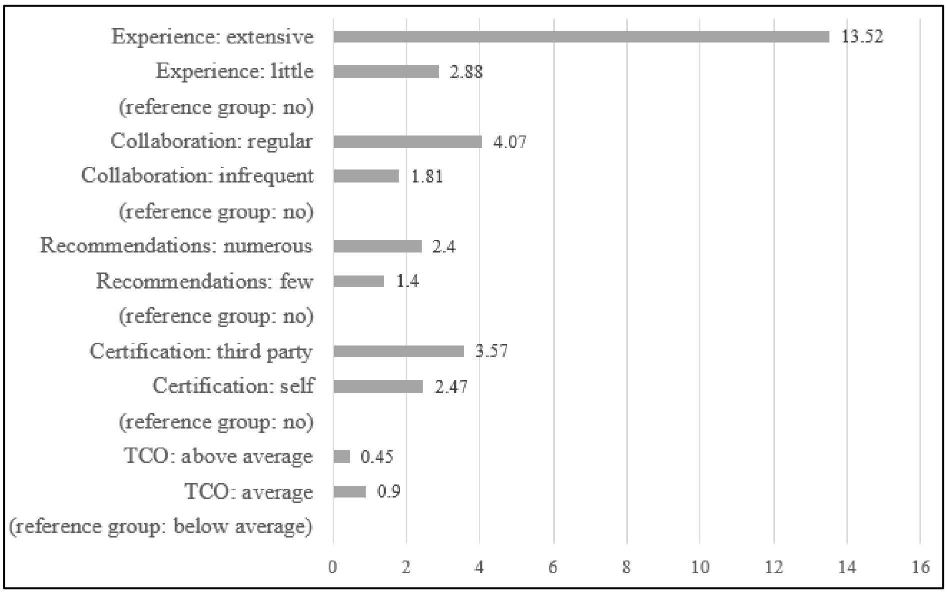


Figure 4-6: Odds ratios of attribute levels

Software suppliers with an extensive experience in relevant areas demonstrate an odds ratio of 13.52. This means they are over 13 times more likely to be chosen compared to a software supplier with no respective experience. This underscores the outstanding importance of this decision attribute. A supplier with which a company has a regular collaboration history possesses a four times higher chance for being selected than one without former collaboration. Numerous recommendations from customers lead to a 2.4 times higher likelihood of a supplier to be chosen (compared to having no recommendations).

4.5.3 Hypothesis testing

Considering all the analyses above, H1a and H1b can be supported. OSS compliance certification accounts for 18.22% of the total utility of a decision maker involved in selecting software suppliers. Being certified for OSS compliance by a third party leads to a three to four times higher likelihood of being chosen compared to having no certification at all. Suppliers with a self-certification still get chosen more than twice as often as the ones not certified. This is comparable to the effect of a supplier having numerous recommendations from previous customers (compared to having no recommendations). As expected, the effect of self-certification is weaker than the one of third-party certification. Yet, it still exists and should not be underestimated.

To examine the influence of self- and third-party certification for OSS compliance on the likelihood of a software supplier being selected in case of the decision maker's awareness of the ISO 5230 standard (H2a and H2b), I calculated the interaction effect between the attribute levels self- and third-party certification and "ISO 5230 awareness". Further, for H3a and H3b, I calculated the interaction effect between the attribute levels self- and third-party certification and "Perceived risk of OSS procurement". Observing interaction effects allows for a deeper understanding of possible heterogeneity of software purchasing experts with regard to their supplier selection decisions. The results of the two logistic regressions are displayed in Table 4-3 (Model 2: interaction with "ISO 5230 awareness"; Model 3: interaction with "Perceived risk of OSS procurement").

Model 2 reveals that H2a can be confirmed. Software purchasing experts who are aware of the ISO 5230 standard assign more value to a self-certification for OSS compliance (0.615, $p < 0.05$) compared to those unfamiliar with the standard. In contrast, H2b cannot be supported. The interaction between ISO 5230 awareness and third-party certification is not significant. Thus, it cannot be concluded that the effect of third-party certification increases when the decision maker is aware of ISO 5230. The Wald test comparing the base model with the interaction model showed a statistically significant improvement for the latter (chi2(3) = 9.41, $p < 0.05$). Hence, the inclusion of the interaction variables seems to increase the model fit.

Model 3 shows that H3b can be supported. The higher is the software purchasing expert's perceived risk of OSS procurement the more he or she values a third-party certification (0.415, $p < 0.05$). In contrast, H3a is not supported. The interaction of perceived risk of OSS procurement and self-certification is not significant, leading to the conclusion that the effect of self-certification is not increased with a higher perceived risk of OSS procurement by the decision maker. Again, the respective Wald test showed a statistically significant improvement for Model 2 compared to the base model (chi2(3) = 10.42, $p < 0.05$), indicating that the inclusion of the interaction increased the model fit. Table 4-4 shows a summary of the hypothesis testing results.

Table 4-4: Summary of hypothesis testing results

Hypothesis	**Supported/Not supported**
H1a	Supported
H1b	Supported
H2a	Supported
H2b	Not supported
H3a	Not supported
H3b	Supported

4.6 Discussion

Regarding the effect of certification on (software) supplier selection, this study builds on earlier research that has found a positive impact (Biong, 2013; Goebel et al., 2018). Yet, prior work focused exclusively on certification by a third party. I additionally consider self-certification as a valuable signal. Results show that OSS compliance third-party certification is superior to self-certification, which in turn is superior to no certification for a software supplier to be selected. The positive effect of self-certification is even increased when customers are aware of the respective ISO standard. When it comes to third-party certification, the positive effect is largely driven by the software purchasing experts' perceived risk of OSS procurement.

My analyses indicate that the positive effect of a self-certification should not be underestimated. In general, its influence is weaker than the one of a third-party certification. Yet, self-certified suppliers still are selected more than twice as often as the ones without certification. This effect is comparable to the one of a supplier having numerous recommendations from former customers (compared to having no recommendations). Hence, self-certification apparently has a large impact on supplier selection and should be considered a valuable signal. This effect is even increased when customers are aware of the respective standard. One rationale behind this result could be that being aware of the standard implies also being aware of the underlying certification procedures and thus increasing their credibility. In the context of this study, this means that companies are familiar with the intended self-certification procedure and can assess the investment associated with a thorough OSS compliance self-certification process, increasing its credibility and signal effectiveness.

Finally, my results show that the positive effect of third-party certification is higher when the software purchasing experts' perceived risk of OSS procurement is high. Apparently, experts with a high perceived risk prefer a third party to independently assess a supplier's OSS compliance measures to reduce the overall perceived risk of the purchasing scenario and be able to use the certification as a way to justify their own selection decision within their own company in case problems related to a lack of OSS compliance occur.

4.7 Implications

4.7.1 Implications for theory

I identify OSS compliance certification as a new and relevant phenomenon in company-involved OSS development. Researchers in this area have put so far a strong focus on certification that targets OSS itself (Feuser & Peleska, 2010; Kakarontzas et al., 2010). This study moves away from a product-focus towards a process-focus by investigating a certification approach targeting companies' underlying OSS compliance processes. In the IT context, the effect of certifications has mainly been investigated in the B2C sector (Kaplan & Nieschwietz, 2003; Nöteberg et al., 2003). By examining the role of an OSS compliance certification in the software supply chain, I extend the perspective to the B2B sector. I identify OSS compliance certification as a valuable signal for software supplier quality showing that it plays a significant role in the selection of software suppliers. In addition, self-certification has proven to be a legitimate alternative to a third-party certification in the OSS compliance context.

Beyond my main contribution to the literature on company-involved OSS development, I also contribute to the literature on signaling and certification (Connelly et al., 2011; Kalliamvakou et al., 2016; Lins & Sunyaev, 2017). To my best knowledge, I am the first to distinguish between self- and third-party certification in this literature stream. More specifically, I introduce self-certification as an example of a valuable nondissipative signal (i.e., a signal that is at first glance not associated with a significant up-front investment but only bears the risk of losing future profits) (Bhattacharya, 1980; Rao et al., 1999). Experts being aware of the respective ISO standard recognize that the self-certification indeed comes along with an upfront investment. Hence, for this group, self-certification even fulfills both traditional requirements of a signal (i.e., signal observability and signal cost). This study adds ISO 5230 awareness and perceived risk of OSS procurement to the list of characteristics of signal receivers that have an influence on how receivers interpret quality signals increasing signal effectiveness (Connelly et al., 2011; Lins & Sunyaev, 2017).

4.7.2 Implications for practice

This study also offers implications for practitioners. First, software suppliers should not underestimate the signaling potential of an OSS compliance certification. Thereby, self-certification is a legitimate alternative to a third-party certification with substantial signaling value. If performed thoroughly, it is still associated with a substantial investment, as usually several employees from different departments are involved in the process. Yet, the overall costs lie below those for a third-party certification, offering a significant saving potential. The risk of losing customers and future profits when it is uncovered that despite self-certification, key requirements of a sound OSS compliance program are in fact not met, should prevent software suppliers from cheating in the self-certification process.

For organizations maintaining ISO standards, one interesting insight is that the awareness of a standard can increase signal effectiveness also for rather uncommon certification approaches (e.g., self-certification). Thus, these organizations should put large efforts into spreading knowledge about standards, especially new unestablished ones. The results of my study encourage the development of self-certification approaches for standards in other areas of software development and procurement, as this study shows that they have a value (albeit lower than the one associated with traditional third-party certification).

4.8 Limitations and avenues for future research

This study is not without limitations. Overall, conjoint experiments have proven to be a suitable method to mimic actual selection processes in which decision makers need to make trade-offs between certain attributes. However, the results can still be affected by the selection of decision makers, the choice of decision-making factors, and construct validity, potentially ignoring other relevant criteria beyond those chosen (Shepherd &

Zacharakis, 2018). I tackle this issue by thoroughly reviewing the literature on supplier selection as well as the signaling theory literature and validating the chosen criteria in expert interviews.

Further, external validity can be an issue in conjoint experiments, as participants face hypothetical decision scenarios. Yet, prior studies have shown that under certain conditions external validity is given for conjoint studies (Shepherd & Zacharakis, 2018). One prerequisite are tasks that reflect real-life decision scenarios as authentically as possible. To ensure this, I performed a pre-test with a software sourcing expert and several colleagues.

The insights from this study are limited to the 105 participants who took part. As the handling of OSS and the perception of OSS compliance potentially may differ between countries, the importance of certain selection criteria, including an OSS compliance certification, might also be subject to geographical differences. Thus, future research should be conducted that replicate my study in other geographical contexts.

Another area for future research lies in the differentiation of early and later phases of the supplier selection process. As previous research has shown, the importance of specific decision criteria depends on the respective decision stage (i.e., consideration stage versus final choice stage) (Blombäck & Axelsson, 2007; Plank & Ferrin, 2002; Wuyts et al., 2009). This study focuses on the final decision stage of the software supplier selection process. Hence, future research could replicate my study focusing on the initial consideration phase to uncover potential differences especially in the perception of an OSS compliance certification.

5 Decision-making patterns in the selection of software suppliers

5.1 Introduction

This exploratory chapter is closely related to the study in chapter 4, as it builds on the same sample. The aim is to discover potential decision-making patterns in the selection of software suppliers and to gain a more differentiated picture about the relevance of the different supplier-related decision criteria, including OSS compliance certification. Thus, I pose the following exploratory research questions: *Based on the decision-making preferences observed in chapter 4, which distinct groups of decision makers can be identified and how can they be characterized? Which individual, firm, and business unit-level factors can predict cluster affiliation?*

To address the first research question (RQ1), I conduct a cluster analysis including hierarchical and non-hierarchical methods with the participants from the study described in chapter 4 to determine different decision maker groups. Subsequently, the relationship between the detected clusters and several individual, firm, and business until-level variables (passive variables) are analyzed in detail to answer the second research question (RQ2).

The cluster analysis reveals four distinct decision maker groups: Experience and OSS compliance certification-focused decision makers, experience and collaboration-focused decision makers, experience-focused decision makers, and OSS compliance certification-focused decision makers.

One-way ANOVA and post-hoc Tukey-Kramer tests are applied to examine whether the clusters depict statistically significant differences in the means of the passive variables of interest. The analyses show that the identified clusters exhibit similarities in several individual-level characteristics. For all clusters, the decision makers’ main tasks include legal issues (means ranging from 3.39 to 4.00) and procurement activities (means ranging from 3.36 to 3.94). They demonstrate experience with OSS (means ranging from 3.45 to 4.00) and OSS compliance (means ranging from 3.41 to 3.59). In contrast, on average, they appear to be less experienced with OSS compliance certification (means ranging from 2.09 to 2.88).

Regarding firm and business unit-level characteristics, the clusters are similar in firm age and size. On average, the business models of the business units possess a rather weak relation with OSS (means ranging from 2.26 to 2.58). Yet, the units appear to be quite intense OSS users (means ranging from 3.94 to 4.24). Across clusters, the business units have a similar OSS compliance maturity. There is a large agreement that not complying with OSS licenses leads to a significant reputational damage (means ranging from 3.56 to 3.77).

Apart from these similarities, the analyses further discover several factors which serve as predictors for cluster affiliation. The first relevant group of such factors are drivers for OSS compliance. The relevance of internal policies, top management, customers, and industry requirements as certification drivers significantly differs across several clusters. In addition, the perceived risk of OSS procurement in general and two specific risks associated with OSS have also been revealed as predicting factors for the clusters: The risk that OSS does not perform to the desired quality and scope and the risk that business units lose their ability to react flexibly to changes in the market through OSS adoption. Finally, the decision makers' experience with software procurement appears to have a prediction value as well.

Based on these findings, it becomes apparent that the four decision maker groups fall into two different categories regarding the aforementioned predictors. Decision makers in clusters 1 and 4 form the category with a high perceived risk of OSS procurement and large relevance of OSS compliance certification drivers. In contrast, decision makers in clusters 2 and 3 belong to the category with a low perceived risk of OSS procurement and low relevance of OSS compliance certification drivers.

5.2 Method

Cluster analysis is an explorative multivariate method suitable to determine groups of decision makers with similar preferences when it comes to decision criteria. The aim is to divide observations into objectively comparable segments based on several active clustering factors in a way that within-cluster homogeneity and between-cluster heterogeneity are maximized (Everitt et al., 2011; Hair et al., 2010; Moyses-Scheingruber, 2020). In this study, the active clustering variables are the average utilities at the individual level of the supplier-related decision criteria used in the previous conjoint experiment (chapter 4): A software supplier's relevant experience, previous collaboration with a software supplier, recommendations from a software supplier's prior customers, and a software supplier's ISO certification for OSS compliance. We left out the total cost of ownership of the offered software, as this is a product-related criterion and we decided to focus on supplier characteristics. To ensure external validity of the clustering result, selecting the active clustering variables needs to be theory driven. Further prerequisites are a sufficiently large sample and no multicollinearity for the active clustering variables

(Hair et al., 2010). As described in the chapters 4.3.1 and 4.3.2, the selected active clustering variables were derived from previous literature and their importance has been confirmed through expert interviews conducted prior to the conjoint study in chapter 4. The correlation matrix in Table 5-1 shows that the clustering variables are not affected by multicollinearity.

Table 5-1: Correlation matrix of active clustering variables

Clustering Variables	(1)	(2)	(3)	(4)
(1) Collaboration	1.000			
(2) Experience	-0.321***	1.000		
(3) Recommendations	0.188	0.052	1.000	
(4) OSS Compliance Certification	-0.571***	-0.435***	-0.514***	1.000

N = 104; Pearson correlation coefficients; *** p<0.001, ** p<0.01, * p<0.05

In sum, cluster analysis constitutes a suitable approach to tackle the first research question and to create an empirical taxonomy of decision-making patterns in the selection of software suppliers (Sabherwal & King, 1995). More specifically, a two-stage clustering approach, including hierarchical and non-hierarchical clustering methods, is applied to generate a reliable cluster structure. This approach is also commonly suggested by prior literature (Hair et al., 2010; Ketchen & Shook, 1996; Milligan & Cooper, 1985; Moyses-Scheingruber, 2020). Concretely, this study first uses the single-linkage approach (to identify and eliminate outliers) and the Ward's minimum variance approach (to define the final number of clusters) as hierarchical clustering methods. Hierarchical clustering represents a bottom-up iterative algorithmic process to create clusters by first regarding each observation as individual cluster. In every following step, two existing clusters with the lowest distance from each other are united until all observations are combined into a single cluster (so-called "chaining") (Everitt et al., 2011; Hair et al., 2010; Moyses-Scheingruber, 2020). The single-linkage approach is also called "nearest neighbor method" and uses the minimum distance from any object in one cluster to any object in another cluster to define the similarity between clusters (Everitt et al., 2011; Rajalahti & Kvalheim, 2011). This method is highly suitable for the detection of outliers, but usually gravitates towards unbalanced, loose cluster solutions due to "chaining" (Everitt et al., 2011; Milligan, 1980). As the following Ward's minimum variance approach is highly sensitive to outliers, prior detection and elimination is crucial (Milligan, 1980).

In the second stage, K-means clustering was performed, which belongs to the non-hierarchical clustering methods. These approaches split the observations into a predefined number of clusters. Observations are iteratively repartitioned into clusters with the closest centroids based on a specific similarity measure, until all observations are optimally assigned (Hair et al., 2010; Ketchen & Shook, 1996). For all methods, the squared Euclidean distance served as similarity measure. It is highly suitable for metric active clustering factors. Moreover, it is the most recommended similarity measure for the Ward's minimum variance and the K-means clustering method (Rajalahti & Kvalheim, 2011).

The core benefit of this two-stage approach is the increase in validity of the final cluster solution, as it balances the downsides and biases of each single method (Everitt et al., 2011; Moyses-Scheingruber, 2020). The Ward's minimum variance clustering approach is usually highly sensitive to outliers (i.e., observations that demonstrate extreme values) (Milligan, 1980). The K-means clustering approach can offset this downside, because it is less sensitive to outliers and to the potential integration of inadequate active clustering factors (Rajalahti & Kvalheim, 2011). Moreover, the Ward's minimum variance clustering approach aims at identifying clusters of similar sizes. This leads to the risk of clusters representing smaller portions of the sample not being detected (Everitt et al., 2011; Rajalahti & Kvalheim, 2011). This downside results from the characteristic of hierarchical clustering methods to not reassign already grouped observations to other clusters. Undesired early cluster creation and seemingly forced results may be the consequence (Rajalahti & Kvalheim, 2011). Additionally applying a non-hierarchical method like K-means clustering to define the final cluster solution helps to balance this limitation. In non-hierarchical approaches, observations can move between clusters until the optimal within-cluster homogeneity and between-cluster heterogeneity are reached (Everitt et al., 2011; Ketchen & Shook, 1996; Moyses-Scheingruber, 2020). Figure 5-1 illustrates the chosen two-stage clustering process.

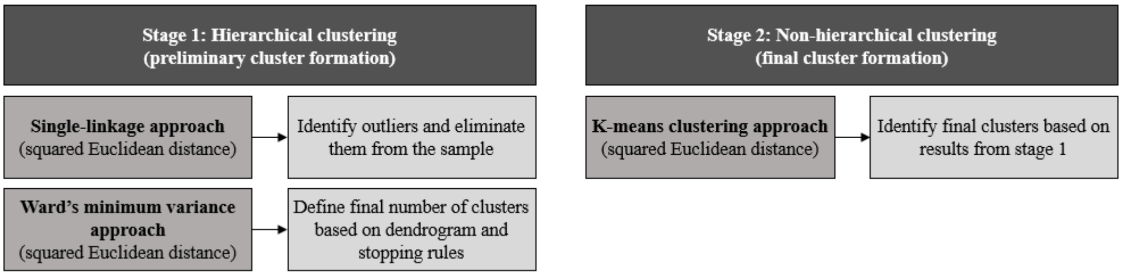

Stage 1: Hierarchical clustering
(preliminary cluster formation)
Single-linkage approach
(squared Euclidean distance)
Identify outliers and eliminate them from the sample
Ward's minimum variance approach
(squared Euclidean distance)
Define final number of clusters based on dendrogram and stopping rules
Stage 2: Non-hierarchical clustering
(final cluster formation)
K-means clustering approach
(squared Euclidean distance)
Identify final clusters based on results from stage 1

Figure 5-1: Two-stage clustering process (based on Moyses-Scheingruber (2020))

5.3 Results

5.3.1 Identification of preliminary cluster solution

First, the single-linkage clustering approach was applied to identify potential outliers for the dataset (n=107). The one participant who displayed “clicking-through” behavior was also excluded prior to this analysis (see chapter 4.4.4.1). Since the analyses in chapter 4, two more participants took part in the study. These additional participants were included here. Based on the resulting dendrogram, a two-dimensional diagram that graphically depicts the clustering outcome, three outliers were identified (G1 to G3; see Figure 5-2). The nodes in the dendrogram represent the clusters. The longer the vertical lines, the more distinct are the respective clusters (Everitt et al., 2011). G1 to G3 appear to be quite different compared to the rest of the observations. This is the reason why they were eliminated from the dataset. Thus, the final dataset consisted of 104 observations.

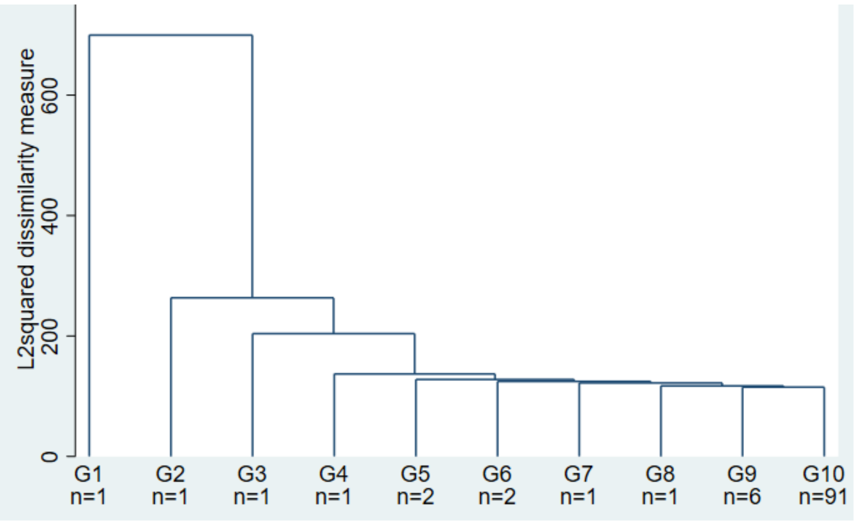


Figure 5-2: Dendrogram for single-linkage clustering approach

The following Ward’s minimum variance approach was used to define the final number of clusters which was needed as input for the final K-means clustering. A first look at the respective dendrogram hinted at a three to four cluster solution (see Figure 5-3). To supplement this purely visual interpretation, two stopping rules were applied. Stopping rules are a more formal way to find out the optimal number of clusters (Everitt et al., 2011; Hair et al., 2010). More concretely, the Calinski and Harabasz pseudo-F index and the Duda and Hart index were calculated. According to prior literature, these two indices are among the stopping rules with very good performance (Everitt et al., 2011; Moyses-Scheingruber, 2020).

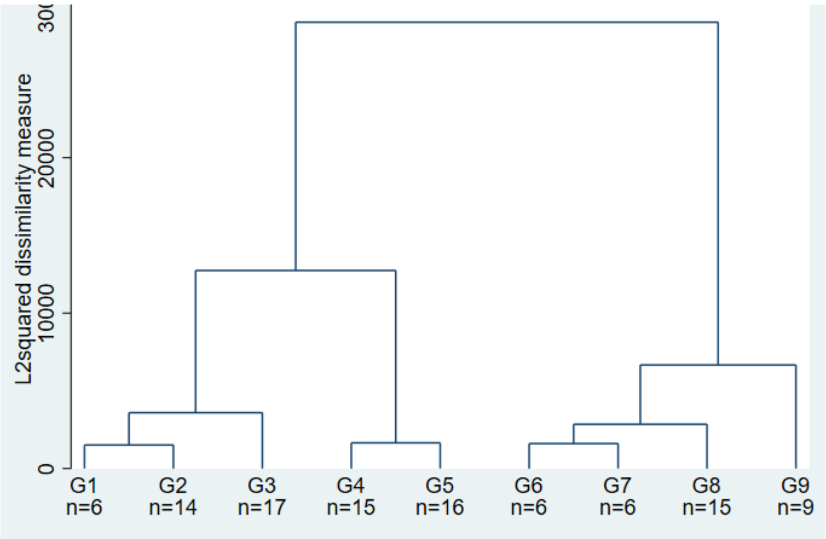
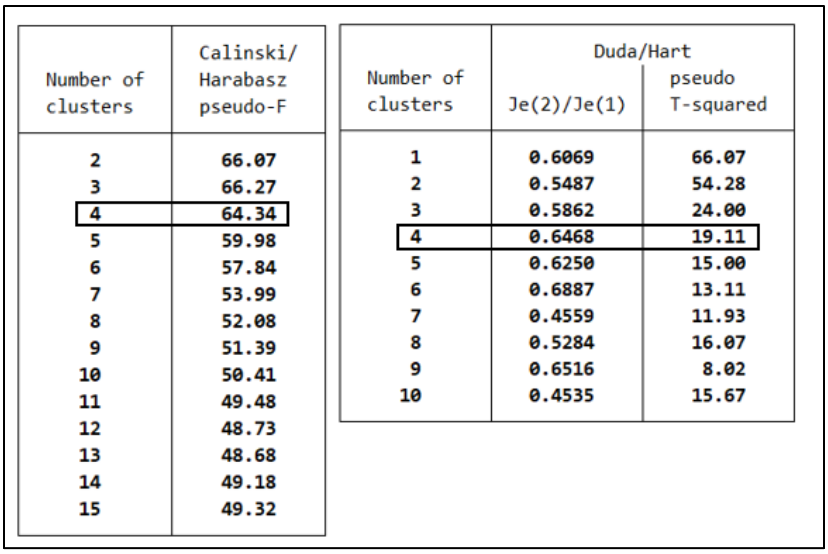


Figure 5-3: Dendrogram for Ward's minimum variance clustering approach

For the Calinski and Harabasz pseudo-F index, the cluster solution with the highest value is perceived optimal. For the Duda and Hart index, one is looking for a high Je(2)/Je(1) value with a low respective pseudo T-squared (Everitt et al., 2011). Looking at the values for the clustering result produced by the Ward’s minimum variance approach, the four-cluster option appears to deliver the most distinct clustering solution. It produces a Calinski and Harabasz pseudo-F value of 64.34. For the Duda and Hart index, the Je(2)/Je(1) value of this solution is 0.6468 with a corresponding pseudo T-squared of 19.11 (see Figure 5-4). For both indices individually, there exist options with better values than the four-cluster solution (e.g., three-cluster solution with a Calinski and Harabasz pseudo-F value of 66.27). Yet, when considering both indices simultaneously, the four-cluster solution appears to be the most suitable option.



Number of clusters	Calinski/ Harabasz pseudo-F
2	66.07
3	66.27
4	64.34
5	59.98
6	57.84
7	53.99
8	52.08
9	51.39
10	50.41
11	49.48
12	48.73
13	48.68
14	49.18
15	49.32

Number of clusters	Duda/Hart Je(2)/Je(1)	pseudo T-squared
1	0.6069	66.07
2	0.5487	54.28
3	0.5862	24.00
4	0.6468	19.11
5	0.6250	15.00
6	0.6887	13.11
7	0.4559	11.93
8	0.5284	16.07
9	0.6516	8.02
10	0.4535	15.67

Figure 5-4: Calinski/Harabasz and Duda/Hart indices

5.3.2 Final cluster solution

Based on the insights from chapter 5.3.1, non-hierarchical clustering was performed using the K-means approach (similarity measure: squared Euclidean distance). This analysis resulted in the final cluster solution revealing four distinct groups of decision makers related to the selection of software suppliers. To test whether the four clusters demonstrate statistically significant differences between the means, a one-way ANOVA was conducted for the product-related attribute “total cost of ownership of the software” which has been left out of the clustering process deliberately. It is important that the respective variable was not part of the clustering process itself, as this would result in a circular and invalid ANOVA (Rabe-Hesketh & Everitt, 2003). As the standard deviations apparently increase with the mean (see Table 5-2), the variable “total cost of ownership of the software” was log-transformed before the ANOVA F-test (Rabe-Hesketh & Everitt, 2003). The ANOVA F-statistics show that the clusters depict statistically significant differences in the average importance of the attribute “total cost of ownership of the software” when selecting a software supplier ($F_{3,100} = 18.52$, $p < 0.001$).

Table 5-2: Means and standard deviations of the importance of the attribute "total cost of ownership of the software" per cluster

Cluster	Mean (TCO)	Standard dev. (TCO)
(1)	7.97	3.48
(2)	15.13	5.30
(3)	8.57	4.08
(4)	17.61	6.73

TCO: total cost of ownership

The cluster analysis result is summarized in Table 5-3. It depicts the average relative importance values of the attributes per cluster. Figure 5-5 provides a graphical representation of the cluster solution. To examine the relationship between the cluster solution and several individual, firm, and business unit-level variables (passive variables), one-way ANOVA was performed. For those variables for which the ANOVA F-test revealed significant differences between the means across clusters ($p < 0.05$), a Tukey-Kramer test was conducted subsequently. The Tukey-Kramer test is a modification of Tukey’s Honest Significant Difference (HSD) range test that is more suitable for unequal cluster sizes (Tukey, 1949). With cluster sizes ranging from N = 17 to N = 33, the Tukey-Kramer test appears to be the more adequate method. It represents a post-hoc pairwise comparison and thus can tell which specific clusters demonstrate statistically significant differences between variable means. This conclusion cannot be drawn when only applying ANOVA. The outcome of the ANOVA F-tests is summarized in Table 5-4 (individual-level variables) and Table 5-5 (firm and business unit-level variables). The results of the Tukey-Kramer tests are documented in Table A-1 (individual-level variables) and Table A-2 (business unit-level variables) in the appendix (pp. 103ff.).

Table 5-3: Result of the K-means clustering analysis with squared Euclidean distance

Attributes	Cluster (1)	Cluster (2)	Cluster (3)	Cluster (4)
Collaboration	8.83	24.06	16.52	18.27
Experience	37.40	30.67	46.94	18.40
Recommendations	12.03	17.43	17.37	12.95
OSS Compliance Certification	33.77	12.71	10.59	32.77
N = 104	22	33	32	17
% of sample	21.15	31.73	30.77	16.35

Notes: The numbers in the table reflect the relative importance values of the attributes. They stem from the average utility estimates derived from a Hierarchical Bayes model. They do not sum up to 100 for each cluster, as the conjoint attribute “total cost of ownership of the software” was not part of the clustering process.

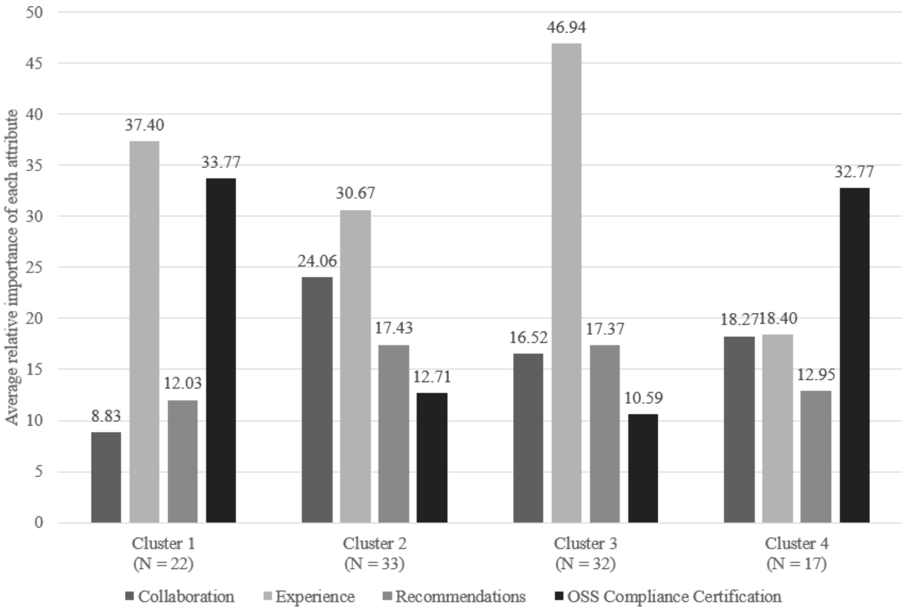


Figure 5-5: Average relative attribute importance for final cluster solution

The identified clusters demonstrate similarities in several individual, firm, and business unit-level characteristics. In all clusters, the decision makers’ main tasks primarily involve legal issues (means ranging from 3.39 to 4.00) and procurement activities (means ranging from 3.36 to 3.94). They possess experience with OSS (means ranging from 3.45 to 4.00) and OSS compliance (means ranging from 3.41 to 3.59). In contrast, on average, they demonstrate less experience with OSS compliance certification (means ranging from 2.09 to 2.88).

Regarding firm and business unit-level characteristics, the clusters are similar in firm age and size. In all clusters, firms demonstrate on average over 30 years of experience. The average number of employees does not demonstrate a statistically significant difference either (between 1,001 and 3,000 employees for cluster 2; between 10,001 and 50,000 employees for cluster 4). On average, the business models of the business units possess a rather weak relation with OSS (means ranging from 2.26 to 2.58). Yet, the units appear to be quite intense OSS users (means ranging from 3.94 to 4.24).

Across clusters, the business units have implemented between four to five OSS compliance measures (maximum possible: 9 measures), hinting at a similar OSS compliance maturity. There is a large agreement that not complying with OSS licenses leads to a significant reputational damage (means ranging from 3.56 to 3.77). The average percentage of business units being OSS compliance certified is not significantly different across clusters. 3 to 12% of the units are self-certified; zero to 5% are certified by a third party. In the following, each of the four clusters is described in detail.

Cluster 1: Experience and OSS compliance certification-focused decision makers

This cluster contains 22 decision makers who base their decision for a software supplier primarily on the supplier's relevant experience (37.4%) and OSS compliance certification (33.77%). Members of this cluster react least sensitively to changes in the attribute "collaboration" (see Figure A-3 in the appendix, p. 105). In contrast, they are very sensitive to changes in the attribute "OSS compliance certification", valuing third-party certification significantly higher than self-certification (see Figure A-6 in the appendix, p. 106).

Cluster 1 demonstrates the largest share of female decision makers (37%). The average age lies between 41 and 50 years. The most represented industry is the ICT sector (50%), followed by manufacturing, transport, and logistics (18%). 41% of the business units are located in Germany. With a mean of 2.98, the decision makers depict the largest value of perceived risk of OSS procurement compared to the other clusters, especially compared to clusters 2 and 3. Their means are statistically significantly different from the one in cluster 1 (see Table A-2 in the appendix, p. 104). In the first cluster, the most important risks associated with OSS are significant reputational and financial losses due to non-compliance with OSS licenses (M = 3.77 and M = 3.68).

Looking at OSS involvement, business units in cluster 1 rank first when it comes to their employees' participation in OSS projects and employees with leading roles in OSS communities (M = 3.32 and M = 3.18). With 64% being familiar with the ISO 5230 standard and 68% with the OpenChain Project, the decision makers depict the largest share of awareness for these topics. 9% are active members of the OpenChain Project, representing the lowest share among all clusters. Regarding the attitude towards OSS compliance certification, members of cluster 1 demonstrate the largest mean value for several factors. Such a certification signals trustworthiness (M = 4.18), organizational quality (M = 4.05), competence (M = 4.00), and a good reputation (M = 4.00). It stands out that several drivers for OSS compliance certification support the significant differentiation of cluster 1 from other clusters, especially from clusters 2 and 3 (see Table A-1 in the appendix, p. 103). Decision makers in cluster 1 on average perceive internal policies (M = 3.50), requirements in the industry sector (M = 3.45), customers (M = 3.45), and the top management (M = 3.32) as most decisive drivers for OSS compliance certification.

Cluster 2: Experience and collaboration-focused decision makers

Cluster 2 represents the largest group. The 33 decision makers mainly focus on a supplier's experience (30.67%) and previous collaboration (24.06%) when selecting software suppliers. In contrast to cluster 1, members of this cluster react most sensitively to changes in the attribute "collaboration" (see Figure A-3 in the appendix, p. 105). Further, compared to cluster 1 and 4, they are very sensitive to changes in the attribute "recommendations" (see Figure A-5 in the appendix, p. 106). When it comes to OSS compliance certification, they perceive self- and third-party certification almost equally (see Figure A-6 in the appendix, p. 106).

85% of the cluster members are male. On average, they are between 41 and 50 years old. With a mean of 2.09, the decision makers have the lowest degree of experience with OSS compliance certification. The same is valid for experience with software procurement (M = 3.39). This factor significantly differentiates cluster 2 from cluster 1 and 4 (see Table A-1 in the appendix, p. 103). 39% of the business units are active in the ICT industry, followed by 15% being active in engineering. Most business units are located in Germany (73%). With a mean of 2.32, the cluster possesses a rather low perceived risk of OSS procurement. Just like in cluster 1, the most relevant risks associated with OSS are significant reputational and financial losses due to non-compliance with OSS licenses (M = 3.76 and M = 3.30).

Regarding OSS involvement, business units in cluster 2 depict the largest means for applying OSS principles internally (M = 3.88), adopting OSS as end users (M = 4.24), and creating and leading own OSS projects (M = 3.61). 55% of the decision makers in cluster 2 are aware of the OpenChain Project, but only 39% know the ISO 5230 standard. 12% are active members of the OpenChain Project. Looking at the attitude towards OSS compliance certification, it stands out that cluster 2 offers the lowest mean value for the statement that such a certification signals a good reputation (M = 3.33). The mean is statistically significantly different from the one of cluster 1 (see Table A-1 in the appendix, p. 103).

Cluster 3: Experience-focused decision makers

The second-largest cluster comprises 32 decision makers. When choosing software suppliers, they base their decision mainly on a supplier's relevant experience (46.94%). This is also reflected in the highest sensitivity towards changes in the attribute "experience" compared to the other clusters (see Figure A-4 in the appendix, p. 105). Moreover, the decision makers are very sensitive to changes in the attribute "recommendations" (see Figure A-5 in the appendix, p. 106). Regarding OSS compliance certification, they possess a similar sensitivity as cluster 2. Yet, there is a larger difference in the perception of self- and third-party certification (see Figure A-6 in the appendix, p. 106).

84% of the decision makers in cluster 3 are male. The average age is 41 to 50 years. They possess the largest experience with OSS (M = 4.00). The primary industries in cluster 3 are the ICT sector (34%), engineering (19%), and manufacturing, transport, and logistics (16%). 84% of the business units are located in Germany, representing the biggest share among all clusters. With a mean of 2.26, the cluster portrays the lowest perceived risk of OSS procurement. It is worth highlighting that the mean of 1.91 for the risk that OSS does not perform to the desired quality and scope is significantly different from the one of cluster 1 (M = 2.59). Thus, this risk supports the significant differentiation of the two clusters.

Regarding OSS involvement, cluster 3 shows the largest mean when it comes to business units combining proprietary software with OSS (M = 4.09). The shares of decision makers who are aware of the ISO 5230 standard and the OpenChain Project are similar (50% and 56%). With 19%, cluster 3 possesses the largest proportion of active members of the OpenChain Project. Moving to the attitude towards OSS compliance certification, the statements that OSS compliance certification signals trustworthiness and organizational quality have the lowest mean in cluster 3 (M = 3.56). Again, several drivers for OSS compliance certification support the cluster differentiation. With the lowest means for internal policies (M = 2.22), top management (M = 2.25), and industry sector (M = 2.25) being relevant drivers, cluster 3 is significantly different to clusters 1 and 4 (see Table A-1 in the appendix, p. 103).

Cluster 4: OSS compliance certification-focused decision makers

With 17 decision makers, cluster 4 represents the smallest group. The main decision criterion when selecting software suppliers is whether the supplier is certified for OSS compliance (32.77%). Members of this cluster are least sensitive to changes in the attribute “experience” (see Figure A-4 in the appendix, p. 105). Just like cluster 1, cluster 4 portrays a high sensitivity towards changes in the attribute “OSS compliance certification”. Yet, the difference in the perception of self- and third-party certification is substantially smaller (see Figure A-6 in the appendix, p. 106).

The share of male decision makers in cluster 4 is 82%. On average, they are 41 to 50 years old. They depict the lowest experience with OSS compliance (M = 3.41), but the largest with software procurement (M = 4.18). The latter is significantly different to the mean of cluster 2, supporting cluster differentiation (see Table A-1 in the appendix, p. 103). With 47%, the dominating industry in cluster 4 is manufacturing, transport, and logistics. 65% of the business units are located in Germany and 12% in the USA. Looking at risks associated with OSS, cluster 4 shows the largest mean for substantial financial losses in case of non-compliance with OSS licenses (M = 4.00). This is also valid for the risk of business units losing their ability to react flexibly to changes in the market through OSS adoption (M = 2.82). This mean is significantly different from the ones in cluster 2 and 3 (see Table A-2 in the appendix, p. 104f.).

Cluster 4 appears to be the one with the members engaging the least with OSS communities. It shows the smallest means when it comes to employees with a leading role in OSS projects (M = 2.59), employees’ participation in OSS projects led by a community (M = 2.65), and business units creating and leading own OSS projects (M = 2.88). Like in cluster 3, the shares of those members being aware of the ISO 5230 standard and the OpenChain Project are quite similar (59% and 53%). With 18%, cluster 4 also possesses a comparable share of active members of the OpenChain Project. Regarding the attitude towards OSS compliance certification, the drivers internal policies, top management, and industry requirements support the differentiation of cluster 4 and 3. Further, compared to cluster 2, decision makers in cluster 4 perceive the certification as moral obligation (M = 2.55 vs M = 3.35) (see Table A-1 in the appendix, p. 103).

Table 5-4: Cluster comparison regarding passive variables (individual level)

Variable	Mean (M)				One-way ANOVA F-test
	Cluster (1)	Cluster (2)	Cluster (3)	Cluster (4)	
Demographics					
Male (in %)	0.63	0.85	0.84	0.82	1.53
Age (in 7 categories)	4.45	4.30	4.00	3.71	2.13
Personal willingness to take risks[1]	3.03	3.04	3.03	3.29	0.93
Job-related variables					
Position (in 13 categories)	7.14	7.58	7.91	8.35	0.48
Degree of job formalization[1]	3.67	3.25	3.30	3.56	2.41
Main tasks					
legal issues[1]	3.68	3.39	3.84	4.00	1.51
programming[1]	2.36	2.94	2.72	2.24	1.47
product development[1]	2.82	3.30	3.13	2.94	0.59
marketing[1]	2.36	2.70	2.28	2.47	0.62
sales[1]	2.32	2.55	2.03	2.12	1.00
procurement[1]	3.59	3.36	3.41	3.94	0.81
Experience with…					
OSS[1]	3.45	3.91	4.00	3.53	2.07
OSS compliance[1]	3.59	3.45	3.56	3.41	0.14
OSS compliance certification[1]	2.86	2.09	2.34	2.88	2.63
software procurement[1]	4.09	3.39	3.78	4.18	4.28**
Awareness of…					
ISO 5230 (in %)	0.64	0.39	0.50	0.59	1.20
OpenChain Project (in %)	0.68	0.55	0.56	0.53	0.43
Active member of OpenChain Project (in %)	0.09	0.12	0.19	0.18	0.41
Attitude towards OSS compliance certification					
It signals trustworthiness[1]	4.18	3.67	3.56	3.76	2.41

Variable	Mean (M)				One-way ANOVA F-test
	Cluster (1)	Cluster (2)	Cluster (3)	Cluster (4)	
It signals organizational quality[1]	4.05	3.79	3.56	3.76	1.43
It signals competence[1]	4.00	3.45	3.47	3.59	2.03
It signals a good reputation[1]	4.00	3.33	3.38	3.65	3.02*
It signals a lack of flexibility[1]	2.45	2.18	2.28	2.47	0.65
It signals a lack of creativity[1]	2.32	1.97	2.34	2.41	1.39
It signals a lack of innovativeness[1]	2.18	2.03	2.28	2.18	0.40
It helps to justify actions towards superiors[1]	3.27	3.12	3.13	3.59	1.28
It legitimizes an organization's operations[1]	3.59	3.15	3.28	3.35	1.12
It is demanded by internal policies[1]	3.50	2.70	2.22	3.41	8.38***
It is demanded by top management[1]	3.32	2.55	2.25	3.12	5.14**
It is demanded by customers[1]	3.45	2.91	2.44	2.88	3.83*
It helps organizations to differentiate themselves from competitors[1]	3.77	3.24	2.94	3.59	3.47*
It is required in the industry sector[1]	3.45	2.64	2.25	3.12	7.29***
It is a moral obligation[1]	3.23	2.55	2.75	3.35	3.36*
It is a legal obligation[1]	3.45	2.64	2.66	3.35	3.51*

Notes: N = 104; ANOVA F-tests were conducted to analyze whether statistically significant differences exist between the means of the four clusters; *** p<0.001, ** p<0.01, * p<0.05; [1]Measured on a 5-point Likert scale

Table 5-5: Cluster comparison regarding passive variables (firm and business unit level)

Variable	Mean				One-way ANOVA F-test
	Cluster (1)	Cluster (2)	Cluster (3)	Cluster (4)	
Firm-level characteristics					
Age (in 4 categories)	3.55	3.30	3.56	3.59	0.95
Number of employees (in 12 categories)	9.18	7.33	8.00	9.76	2.61
Annual gross revenues (in 10 categories)	8.05	7.42	8.16	8.59	0.80

Variable	Mean				One-way ANOVA F-test
	Cluster (1)	Cluster (2)	Cluster (3)	Cluster (4)	
BU-level characteristics					
Number of employees (in 9 categories)	6.05	4.94	5.38	6.47	1.75
Industry					
Banking & Financial Services (in %)	0.09	0.09	0.03	0.18	0.99
Consulting & Strategy (in %)	0.05	0.03	0.06	0.06	0.13
Engineering (in %)	0.05	0.15	0.19	0.06	1.10
Healthcare & Medical (in %)	0.05	0.09	0.03	0.00	0.78
ICT (in %)	0.50	0.39	0.34	0.12	2.20
Manufacturing, Transport & Logistics (in %)	0.18	0.06	0.16	0.47	4.71**
Mining, Resources & Energy (in %)	0.00	0.06	0.03	0.06	0.51
Location					
Germany (in %)	0.41	0.73	0.84	0.65	4.28**
Switzerland (in %)	0.00	0.06	0.09	0.00	1.18
United Kingdom (in %)	0.14	0.00	0.00	0.06	2.96*
USA (in %)	0.14	0.06	0.03	0.12	0.84
India (in %)	0.18	0.03	0.00	0.06	3.02*
Attitude towards OSS					
Relation of business model with OSS[1]	2.58	2.56	2.52	2.26	0.39
# of areas of OSS implementation into products/services (from 0 to 4)	1.77	1.64	1.91	1.71	0.51
# of areas of OSS usage (from 0 to 7)	2.86	3.55	3.81	3.71	1.36
Number of implemented OSS compliance measures (from 0 to 9)	5.41	4.3	4.75	4.47	0.76
Perceived risk of OSS procurement[1]	2.98	2.32	2.26	2.82	4.12**
Risks associated with OSS					
OSS does not perform to the desired quality and scope[1]	2.59	2.27	1.91	2.47	2.75*
OSS is not interoperable with existing applications[1]	2.86	2.45	2.5	2.71	0.97
OSS adoption causes unanticipated costs[1]	3.09	2.85	2.56	3.00	1.37
Not complying with OSS licenses leads	3.68	3.30	3.16	4.00	2.33

Variable	Mean				One-way ANOVA F-test
	Cluster (1)	Cluster (2)	Cluster (3)	Cluster (4)	
to a significant financial loss[1]					
Through OSS adoption, the BU loses its ability to react flexibly to changes in the market[1]	2.18	1.85	1.84	2.82	4.66**
Through OSS adoption, the BU highly depends on the OSS community or the vendor of the software[1]	3.32	2.91	3.09	3.24	0.77
Through OSS adoption, the BU loses know-how required to remain competitive[1]	2.36	1.97	1.75	2.18	2.50
Not complying with OSS licenses leads to a significant reputational damage[1]	3.77	3.76	3.56	3.59	0.28
The confidentiality and security of business data are not guaranteed when adopting OSS[1]	3.00	2.36	2.22	2.53	2.37
OSS involvement					
The BU applies OSS principles internally (e.g., inner source)[1]	3.55	3.88	3.81	3.59	0.66
The BU uses OSS in its operational environment as end user[1]	4.00	4.24	4.19	3.94	0.60
The BU combines proprietary software with OSS[1]	3.86	3.76	4.09	3.88	0.67
The BU creates and leads own OSS projects[1]	3.32	3.61	3.25	2.88	1.37
Many BU employees participate in OSS projects led by a community[1]	3.32	3.27	3.13	2.65	1.18
Many BU employees are leading members of OSS communities[1]	3.18	2.67	2.59	2.59	1.28
OSS compliance certification of BU					
Self-certified (in %)	0.09	0.09	0.03	0.12	0.48
Third-party certified (in %)	0.05	0.03	0.00	0.00	0.65

Notes: N = 104; ANOVA F-tests were performed to analyze whether statistically significant differences exist between the means of the four clusters; *** p<0.001, ** p<0.01, * p<0.05; [1]Measured on a 5-point Likert scale

5.4 Discussion

This chapter has the goal to reveal potential decision-making patterns for the selection of software suppliers and to identify certain individual, firm, and business unit-level factors that can predict cluster affiliation. The two-stage cluster analysis shows that the decision makers can be grouped into four distinct clusters with differing decision-making behavior when selecting software suppliers (RQ1): Experience and OSS compliance certification-focused decision makers, experience and collaboration-focused decision makers, experience-focused decision makers, and OSS compliance certification-focused decision makers. The four groups differ regarding the relevance of certain supplier-related characteristics in the software supplier selection process.

Subsequent one-way ANOVA and Tukey-Kramer tests identify certain factors as predictors for cluster structure (RQ2). Among them were certain drivers for OSS compliance. The relevance of internal policies, top management, customers, and industry requirements as certification drivers significantly differs across several clusters. In addition, the perceived risk of OSS procurement in general and two specific risks associated with OSS have also been revealed as predicting factors for cluster affiliation: The risk that OSS does not perform to the desired quality and scope and the risk that business units lose their ability to react flexibly to changes in the market through OSS adoption. Finally, the decision makers’ experience with software procurement appears to have a prediction value as well.

With this said, it becomes apparent that the four decision maker groups fall into two different categories regarding the aforementioned predictors. Decision makers in clusters 1 and 4 demonstrate rather large values for experience with software procurement compared to clusters 2 and 3. Further, they attribute greater importance to the certification drivers internal policies, top management, and industry requirements (customers: only cluster 1). Finally, decision makers in clusters 1 and 4 on average depict higher levels of perceived risk of OSS procurement in general. Looking at the two specific risks identified as predictors, cluster 1 assigns significantly higher relevance to the risk that OSS does not perform to the desired quality and scope than cluster 3. Similarly, cluster 4 assigns significantly higher relevance to the risk that business units lose their ability to react flexibly to changes in the market through OSS adoption compared to clusters 2 and 3. Hence, clusters 1 and 4 fall into the category of decision makers with a high perceived risk of OSS procurement and large relevance of OSS compliance certification drivers. In contrast, clusters 2 and 3 form the category of decision makers with a low perceived risk of OSS procurement and low relevance of OSS compliance certification drivers. Figure 5-6 illustrates the cluster structure.

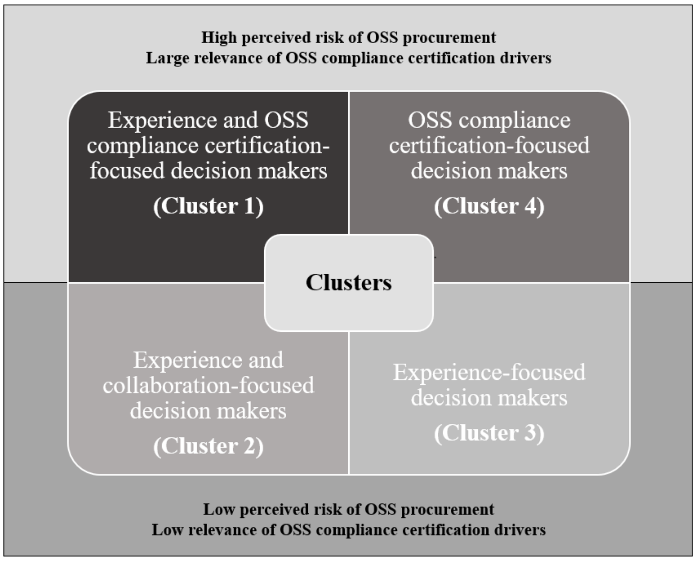

High perceived risk of OSS procurement
Large relevance of OSS compliance certification drivers
Experience and OSS compliance certification-focused decision makers
(Cluster 1)
OSS compliance certification-focused decision makers
(Cluster 4)
Clusters
Experience and collaboration-focused decision makers
(Cluster 2)
Experience-focused decision makers
(Cluster 3)
Low perceived risk of OSS procurement
Low relevance of OSS compliance certification drivers

Figure 5-6: Summary of identified clusters

6 Summary and outlook

6.1 Findings and theoretical contributions

The aim of this dissertation was twofold. First, it aimed at shedding light on how companies handle the topic OSS contribution governance when actively engaging with OSS communities. The second goal was to investigate how companies cope with the topic OSS compliance when using OSS internally, implementing OSS into own products and services, and when acquiring software containing OSS components from suppliers. In this context, the recent phenomenon of OSS compliance certification was exploited.

OSS is gaining relevance for companies of all sizes and industries. Active collaboration with OSS communities comes along with certain challenges for companies. Both parties show diverging interests and ideologies that somehow need to be balanced to enable successful interaction (O'Mahony & Bechky, 2008). OSS communities need to guarantee that all participating parties comply with their requirements and are aligned with the community objectives, whereas companies aim at minimizing the risk of inappropriate knowledge spillovers, protecting company reputation, which may be hurt by low-quality contributions, and avoiding violation of IP rights. Thus, the collaboration requires governance of community as well as company activities (Dahlander & Magnusson, 2008).

For companies, it is essential to set up appropriate governance mechanisms and incentives that manage their employees’ interaction with OSS communities (S. Daniel, Maruping, et al., 2018; Mehra et al., 2011). Yet, when introducing certain internal governance processes, companies face a significant trade-off. They need to ensure a compliant behavior towards the OSS communities, while enabling their organizational units to manage the specific contributions to OSS communities with a certain degree of flexibility. We lacked insights into how companies design mechanisms to govern contributions to OSS communities, while taking this trade-off into account. Chapter 2 picked up this issue and posed the following research question: *How do companies negotiate the trade-off between control and flexibility regarding their employees’ OSS community interaction?*

I approached this research question in a multiple case study (Yin, 2009) at Siemens AG with different organizational units as units of analysis. Siemens has recently set up a template OSS contribution process which the organizational units can adapt to their specific needs. Analyzing how the units adopt the template process and thereby define the flexibility for the developers offers the opportunity to find out how companies negotiate the tensions between control and flexibility by means of governance mechanisms.

Based on twelve interviews with employees who work on OSS-related topics (e.g. software developers, experts for third party software, and managers) and archival data, I found that the extent to which the template process is implemented depends on the following characteristics of the organizational units: the level of closeness to core IP of the unit and the intensity of the involvement in OSS communities (i.e. number and type of contributions, number of OSS communities the unit is involved in). Further, I could show that trust in the employees' technical skills and their OSS experience is essential for granting a certain flexibility for their engagement in OSS communities. Finally, in isolated cases where contributions happen very rarely and the closeness to core IP is low, developers set up a workaround instead of establishing a formal process.

This research contributes to the literature on company-involved OSS development (Ågerfalk & Fitzgerald, 2008; S. Y. Ho & Rai, 2017; Rolandsson et al., 2011), to the IT governance literature (Eaton et al., 2015; Ghazawneh & Henfridsson, 2013; Svahn et al., 2017; Wareham et al., 2014), and more concretely to the OSS contribution governance literature (Germonprez et al., 2017; Germonprez et al., 2012; O'Mahony & Ferraro, 2007) by showing how companies manage their employees' community interaction by means of governance mechanisms.

Governance is not only required when companies interact actively with OSS communities, but also when they use OSS internally or implement it into own products and services. When doing so, companies especially need to ensure that they comply with the obligations that come along with the different OSS licenses (Morgan et al., 2013). Inadequately managed OSS compliance can result in litigations, leading to significant financial and reputational losses for companies (Harutyunyan, 2020). To avoid such conflicts, companies increasingly realize the importance of the topic OSS compliance. Yet, managing compliance is complex, especially when companies acquire software that contains OSS components from external software suppliers. The ISO 5230 standard for OSS compliance and the related self- and third-party certification approaches were specifically developed to help software suppliers in credibly demonstrating their OSS compliance to their customers and other stakeholders. Chapters 3, 4, and 5 were dedicated to the recent phenomenon of OSS compliance certification in the software supply chain.

The study in chapter 3 aimed at answering the following research questions: *Which drivers for OSS compliance certification exist? What motivates or prevents* *companies from attaining OSS compliance certification (self-certification or third-party certification)?*

I performed a multiple case study based on the thematic coding procedure introduced by Flick (2022). In total, 17 semi-structured interviews were conducted with representatives from companies that were either self-certified or certified by a third party and with representatives from third-party certification bodies that offer OSS compliance certification.

Results revealed customers as the largest external driver for self-certified and third-party certified companies. Certification bodies regard regulation as most relevant external driver. From an internal perspective, the increasing relevance of OSS for companies is the most decisive driver for all three groups. Regarding general motives for OSS compliance certification, all three groups name the ability to use it as evidence for OSS compliance in negotiations as most crucial factor. Self- and third-party certified companies thereby mostly refer to negotiations with customers, whereas certification bodies focus on acquisition scenarios. When it comes to specific motives for self-certification, using the ISO standard as benchmark was mentioned most frequently, mostly to cross-check existing OSS compliance processes, but also to design processes from scratch. The most relevant motive for third-party certification across all three groups is the unbiased assessment of OSS compliance by an independent third party. Finally, the generic nature of the ISO standard is not only perceived as advantage, but also as downside. Due to the general formulation, firms sometimes struggle to translate the standard into working processes and certifiers lack guidance regarding which processes to consider as certifiable.

With this study, I contribute to the literature on ISO certification (Anderson et al., 1999; T. Y. Lee, 1998; Quirós & Justino, 2013) by adding significant insights on internal certification drivers. In the case of ISO 5230 certification, committed employees and the increasing relevance of the topic OSS compliance for companies make companies seek certification. Moreover, I add the new perspective of distinguishing between self-certification and third-party certification. Using the ISO standard as benchmark, the equal perception of self- and third-party certification, as well as the availability of the necessary competencies inside the company stand out as relevant motives for self-certification. In contrast, the assessment of OSS compliance measures by an independent third party is the most important factor speaking for third-party certification.

Chapter 4 dealt with the question of how this certification is perceived by firms when selecting software suppliers. I investigated the importance of certification as a criterion in the decision to select a software supplier and distinguish between no certification, self-certification, and third-party certification. I built on signaling theory to theorize how OSS compliance certification can help to overcome information asymmetries between the supplier and acquirer of software. Taking on the signal receiver's perspective, I formulated hypotheses on the role of a software supplier's OSS compliance certification relative to other selection criteria known to be effective signals for supplier quality. I also hypothesized different perceptions of self-certification vs third-party certification as well as moderating factors that might explain potential differences in perception.

Empirically, this study built on a discrete choice-based conjoint experiment (Louviere & Woodworth, 1983), in which real-world software purchasing experts were asked to choose between offers from different software suppliers that all contain OSS components. The design of the conjoint experiment, specifically the selection of the decision criteria, was based on interviews with experts regularly involved in the selection of software suppliers.

The analyses revealed that OSS compliance certification is a decision-relevant criterion for selecting a software supplier. Its relative importance in the sourcing decision is comparable to first-hand experience with suppliers through previous collaboration. A comparison of self- with third-party certification showed that software suppliers with third-party certification are chosen about 2.5 times more likely than self-certified suppliers. Awareness of the regulatory standard ISO 5230 and the perceived risk of OSS procurement are critical moderating factors. Being aware of the ISO 5230 standard significantly increased the positive effect of self-certification, resulting in a reduced gap between the two forms of certification. The perceived risk of OSS procurement increased the positive effect of third-party certification. It had, however, no influence on the effect of self-certification.

Chapter 5 used the sample from the previous conjoint experiment to discover potential decision-making patterns in the selection of software suppliers and to gain a more differentiated picture about the relevance of the different supplier-related decision criteria, including OSS compliance certification. The corresponding exploratory research questions were: *Which distinct groups of decision makers in the selection of software suppliers can be identified and how can they be characterized? Which individual, firm, and business unit-level factors can predict cluster affiliation?*

To address the first research question, I conducted a cluster analysis including hierarchical and non-hierarchical methods. Subsequently, the relationship between the detected clusters and several individual, firm, and business until-level variables (passive variables) were analyzed in detail to answer the second research question. The cluster analysis revealed four distinct decision maker groups: Experience and OSS compliance certification-focused decision makers, experience and collaboration-focused decision makers, experience-focused decision makers, and OSS compliance certification-focused decision makers.

One-way ANOVA and post-hoc Tukey-Kramer tests were applied to examine whether the clusters depict statistically significant differences in the means of the passive variables of interest. The analyses showed that the identified clusters exhibit similarities in several individual-level characteristics. For all clusters, the decision makers’ main tasks include legal issues (means ranging from 3.39 to 4.00) and procurement activities (means ranging from 3.36 to 3.94). They demonstrate experience with OSS (means ranging from 3.45 to 4.00) and OSS compliance (means ranging from 3.41 to 3.59). In contrast, on average, they appear to be less experienced with OSS compliance certification (means ranging from 2.09 to 2.88). Regarding firm and business unit-level characteristics, the clusters are similar in firm age and size. On average, the business models of the business units possess a rather weak relation with OSS (means ranging from 2.26 to 2.58). Yet, the units appear to be quite intense OSS users (means ranging from 3.94 to 4.24). Across clusters, the business units have a similar OSS compliance maturity. There is a large agreement that not complying with OSS licenses leads to a significant reputational damage (means ranging from 3.56 to 3.77).

Apart from these similarities, the analyses further discovered several factors which serve as predictors for cluster affiliation. The first relevant group of such factors are drivers for OSS compliance. The relevance of internal policies, top management, customers, and industry requirements as certification drivers significantly differs across several clusters. In addition, the perceived risk of OSS procurement in general and two specific risks associated with OSS have also been revealed as predicting factors for the clusters: The risk that OSS does not perform to the desired quality and scope and the risk that business units lose their ability to react flexibly to changes in the market through OSS adoption. Finally, the decision makers’ experience with software procurement appears to have a prediction value as well.

The findings from both chapters offer relevant implications for theory. First, the literature on OSS certification is so far focused on certifying OSS itself, reflecting a strong product-orientation (Feuser & Peleska, 2010; Kakarontzas et al., 2010). The approach examined in chapters 4 and 5 aims at certifying underlying OSS compliance processes instead. Hence, I add a new perspective to this literature stream. In IS research, the effect of software certifications has been primarily investigated in the B2C sector (Kaplan & Nieschwietz, 2003; Nöteberg et al., 2003). My two studies examine the concept of OSS compliance certification in the software supply chain and thus transfer the issue of certification to the B2B sector. Second, beyond my main contribution to the literature on company-involved OSS development, I also contribute to the signaling and certification literature (Connelly et al., 2011; Kalliamvakou et al., 2016; Lins & Sunyaev, 2017). I add ISO 5230 awareness and perceived risk of OSS procurement as boundary conditions of signal receivers that influence how receivers interpret certain signals. Further, to the best of my knowledge, I am the first to distinguish between self-certification and third-party certification in this literature stream.

6.2 Practical implications

The four research projects in this dissertation offer several implications for practitioners. Starting with the study in chapter 2, findings indicate that providing flexibility to organizational units in adopting contribution processes to accommodate their specifics is essential for companies. Simply dictating a process might decrease the employees' willingness and ability to engage with OSS communities. Hence, companies might profit less from the involvement, as they are not able to keep up with the fast OSS environment anymore. Second, granting developers particular facilitations based on technical skills and the experience in interacting with OSS communities is a suitable way to provide each of them individually with a certain degree of flexibility in their community engagement.

For companies that think about seeking certification according to the ISO 5230 standard, chapter 3 provides insights into potential advantages and downsides. The study might support companies in their decision whether to strive for self- or third-party certification or to not seek certification at all. Through this study, organizations maintaining ISO standards gain knowledge about what motivates companies to achieve ISO certification and what hinders them. Moreover, they should take into account the ambiguous perception of the generic nature of most ISO standards and provide companies with further material to enable them to translate the standards into processes that fulfill the standard requirements and fit to the company environment.

Chapters 4 and 5 also result in several implications for practitioners. First, software suppliers should not underestimate the signaling potential of an OSS compliance certification in the software supply chain. Self-certification appears to be a legitimate alternative to a third-party certification with substantial signaling value. If performed thoroughly, it is still associated with a substantial investment, as usually several employees from different departments are involved in the process. Yet, the overall costs lie below those for a third-party certification, offering a significant saving potential. The risk of losing customers and future profits when it is uncovered that despite self-certification, key requirements of a sound OSS compliance program are in fact not met, should prevent software suppliers from cheating in the self-certification process.

For organizations maintaining ISO standards, one interesting insight is that the awareness of a standard can increase signal effectiveness also for rather uncommon certification approaches (e.g., self-certification). Thus, these organizations should put large efforts into spreading knowledge about standards, especially new unestablished ones. The results encourage the development of self-certification approaches for standards in other areas of software development and procurement, as my research shows that they indeed have a value (albeit lower than the one associated with traditional third-party certification).

6.3 Limitations and avenues for future research

The research projects in this dissertation are not without limitations and thus provide several opportunities for future research. Regarding chapter 2, I have specifically chosen various organizational units at Siemens for my multiple case study, as OSS plays a significant role for the company as a whole, whereas each unit deals with it differently. However, the fact that I focused on units in one single company challenges the validity of the findings. Therefore, the topic should be investigated in further companies with differing characteristics (e.g., size, industry, location). This would also help to strengthen the finding of this study that the two key dimensions are really the most important factors when companies decide about the governance processes related to their employees' OSS community engagement. Although one could think of further aspects influencing a company's decision between control and flexibility with regard to the OSS contribution process design (e.g., business model, maturity of the software), they did not become apparent in my multiple case study at Siemens.

Moreover, the insights from this study are highly context-specific, meaning that they apply for companies that interact with OSS communities. Hence, it would be worth looking at contexts which involve other co-creation ecosystems (e.g., platform ecosystems) to find out if the findings match. Finally, investigating further organizational units at Siemens, especially those with a high level of closeness to core IP and high intensity of involvement in OSS communities, would help to get an even broader view on the process adoption approaches. I am lacking observations for this specific configuration. One reason could be that only few (or even no) organizational units exist that have a strong closeness to core IP and are still highly involved with OSS communities, as the fear of unintendedly disclosing core IP prevails.

Looking at chapter 3, the unbalanced sample regarding self- and third-party certified companies is an issue. While I could reach twelve companies that are self-certified or are currently in the self-certification process, I was only able to speak to one representative from a single third-party certified company, which makes it difficult to gain comprehensive insights for this group. Hence, gathering additional data from third-party certified firms would lead to a more balanced picture of the results and increase their generalizability.

Moreover, when interpreting the results, it should be taken into account that the majority of the interviewees in the group of self-certified companies were highly involved in the OpenChain Project and thus very committed to the topic OSS compliance. Therefore, it is very likely that these interviewees per se have a more positive attitude towards OSS compliance certification in general and more specifically, towards self-certification. Finally, as the ISO 5230 standard has only been introduced by the end of 2020 and is not yet well-established, future research should examine the drivers and motives for certification several years later to find out whether they change over time. Especially when it comes to the perception of self- and third-party certification, a significant difference is expected in the future. With the standard becoming more popular across different industries, the demand for third-party certification from stakeholders (e.g., customers) will probably increase, especially in highly regulated industries.

The conjoint experiment in chapter 4 comes along with method-related limitations. The results can be affected by the selection of decision makers, the choice of decision-making factors, and construct validity, potentially ignoring other relevant criteria beyond those chosen (Shepherd & Zacharakis, 2018). I tackled this issue by thoroughly reviewing the literature on supplier selection as well as the signaling theory literature and validating the chosen criteria in expert interviews. Further, external validity can be an issue in conjoint experiments, as participants face hypothetical decision scenarios. Yet, prior studies have shown that under certain conditions external validity is given for conjoint studies (Shepherd & Zacharakis, 2018). One prerequisite are tasks that reflect real-life decision scenarios as authentically as possible. To ensure this, I performed a pre-test with a software sourcing expert and several colleagues.

One limitation that is also valid for chapter 5 is that the insights are limited to those participants who took part. The majority came from Germany. As the handling of OSS and the perception of OSS compliance potentially may differ between countries, the importance of certain selection criteria, including an OSS compliance certification, might also be subject to geographical differences. Hence, future research should be conducted that replicate my study in other geographical contexts.

Another area for future research lies in the differentiation of early and later phases of the supplier selection process. As previous research has shown, the importance of specific decision criteria depends on the respective decision stage (i.e., consideration stage versus final choice stage) (Blombäck & Axelsson, 2007; Plank & Ferrin, 2002; Wuyts et al., 2009). My conjoint study focused on the final decision stage of the software supplier selection process. Thus, future research should replicate the study focusing on the initial consideration phase to uncover potential differences especially in the perception of an OSS compliance certification.

Overall, this dissertation delivers first valuable insights on how companies handle the topic OSS contribution governance when actively collaborating with OSS communities. In addition, it sheds light on how companies deal with OSS compliance by exploiting the recent phenomenon of OSS compliance certification in the software supply chain. Yet, in the realm of OSS contribution governance, OSS compliance, and OSS compliance certification, there remain many opportunities for future research. I am confident that this dissertation can serve as starting point and encourages future investigations in this area.

Appendix

A-1: Tukey-Kramer post-hoc test (individual-level variables)

Variable	Cluster comparison (cluster i vs cluster j)	Mean difference (i - j)	Tukey-Kramer t
Experience with software procurement[1]	1 vs 2	0.70	4.12*
	1 vs 3	0.31	1.82
	1 vs 4	-0.09	0.43
	2 vs 3	-0.39	2.54
	2 vs 4	-0.79	4.26*
	3 vs 4	-0.40	2.14
Attitude towards OSS compliance certification			
It signals a good reputation[1]	1 vs 2	0.67	3.86*
	1 vs 3	0.62	3.60
	1 vs 4	0.35	1.74
	2 vs 3	-0.05	0.27
	2 vs 4	-0.32	1.68
	3 vs 4	-0.27	1.44
It is demanded by internal policies[1]	1 vs 2	0.80	3.90*
	1 vs 3	1.28	6.18***
	1 vs 4	0.09	0.37
	2 vs 3	0.48	2.58
	2 vs 4	-0.71	3.20
	3 vs 4	-1.19	5.31**
It is demanded by top management[1]	1 vs 2	0.77	3.61
	1 vs 3	1.07	4.97**
	1 vs 4	0.20	0.80
	2 vs 3	0.30	1.53
	2 vs 4	-0.57	2.47
	3 vs 4	-0.87	3.72*
It is demanded by customers[1]	1 vs 2	0.54	2.58
	1 vs 3	1.01	4.78**
	1 vs 4	0.57	2.31
	2 vs 3	0.47	2.48
	2 vs 4	0.03	0.12
	3 vs 4	-0.44	1.93
It helps organizations to differentiate themselves from competitors[1]	1 vs 2	0.53	2.70
	1 vs 3	0.83	4.22*
	1 vs 4	0.18	0.80
	2 vs 3	0.30	1.72
	2 vs 4	-0.35	1.62
	3 vs 4	-0.65	3.04
It is required in the industry sector[1]	1 vs 2	0.81	4.23*
	1 vs 3	1.20	6.19***
	1 vs 4	0.33	1.48
	2 vs 3	0.39	2.22
	2 vs 4	-0.48	2.29
	3 vs 4	-0.87	4.11*
It is a moral obligation[1]	1 vs 2	0.68	3.40
	1 vs 3	0.48	2.37
	1 vs 4	-0.12	0.53
	2 vs 3	-0.20	1.13
	2 vs 4	-0.80	3.72*
	3 vs 4	-0.60	2.76
It is a legal obligation[1]	1 vs 2	0.81	3.60
	1 vs 3	0.79	3.49
	1 vs 4	0.10	0.38
	2 vs 3	-0.02	0.10

Variable	Cluster comparison (cluster i vs cluster j)	Mean difference (i - j)	Tukey-Kramer t
	2 vs 4	-0.71	2.91
	3 vs 4	-0.69	2.81

Notes: N = 104; Tukey-Kramer post-hoc tests were conducted to reveal statistically significant differences in the variable means of specific clusters; *** p<0.001, ** p<0.01, * p<0.05; [1]Measured on a 5-point Likert scale

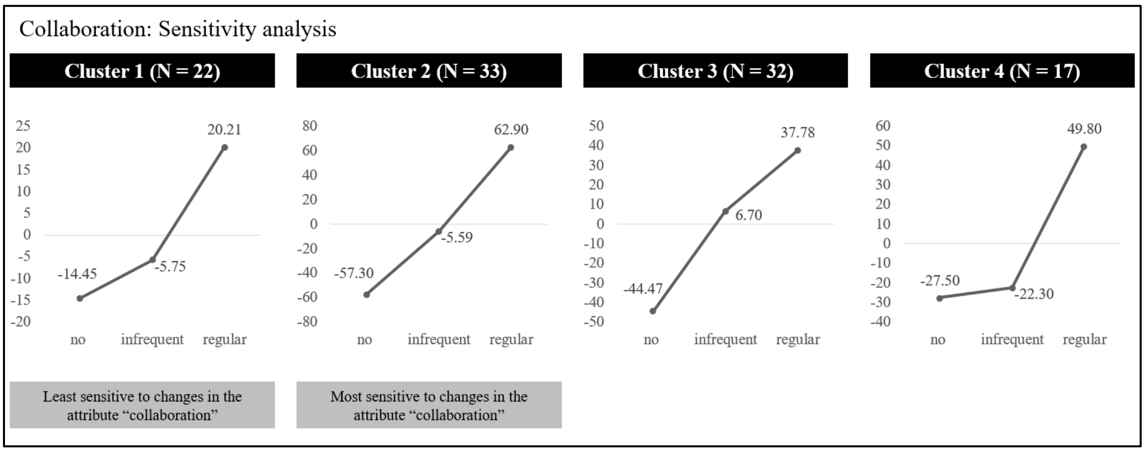
A-2: Tukey-Kramer post-hoc test (business unit-level variables)

Variable	Cluster comparison (cluster i vs cluster j)	Mean difference (i - j)	Tukey-Kramer t
BU-level characteristics			
Industry			
Manufacturing, Transport & Logistics (in %)	1 vs 2	0.12	1.69
	1 vs 3	0.02	0.35
	1 vs 4	-0.29	3.43
	2 vs 3	-0.10	1.48
	2 vs 4	-0.41	5.27**
	3 vs 4	-0.31	4.02*
Location			
Germany (in %)	1 vs 2	-0.32	3.66
	1 vs 3	-0.43	4.97**
	1 vs 4	-0.24	2.33
	2 vs 3	-0.11	1.49
	2 vs 4	0.08	0.85
	3 vs 4	0.19	2.07
United Kingdom (in %)	1 vs 2	0.14	3.73*
	1 vs 3	0.14	3.71*
	1 vs 4	0.08	1.81
	2 vs 3	0.00	0.00
	2 vs 4	-0.06	1.48
	3 vs 4	-0.06	1.47
India (in %)	1 vs 2	0.15	3.42
	1 vs 3	0.18	4.08*
	1 vs 4	0.12	2.37
	2 vs 3	0.03	0.76
	2 vs 4	-0.03	0.59
	3 vs 4	-0.06	1.22
Attitude towards OSS			
Perceived risk of OSS procurement[1]	1 vs 2	0.66	3.82*
	1 vs 3	0.72	4.17*
	1 vs 4	0.16	0.80
	2 vs 3	0.06	0.40
	2 vs 4	-0.50	2.67
	3 vs 4	-0.56	3.00
Risks associated with OSS			
OSS does not perform to the desired quality and scope[1]	1 vs 2	0.32	1.75
	1 vs 3	0.68	3.75*
	1 vs 4	0.12	0.57
	2 vs 3	0.36	2.24
	2 vs 4	-0.20	1.01
	3 vs 4	-0.56	2.85
Through OSS adoption, the BU loses its ability to react flexibly to changes in the market[1]	1 vs 2	0.33	1.76
	1 vs 3	0.34	1.78
	1 vs 4	-0.64	2.90
	2 vs 3	0.01	0.03

Variable	Cluster comparison (cluster i vs cluster j)	Mean difference (i - j)	Tukey-Kramer t
	2 vs 4	-0.97	4.76**
	3 vs 4	-0.98	4.76**

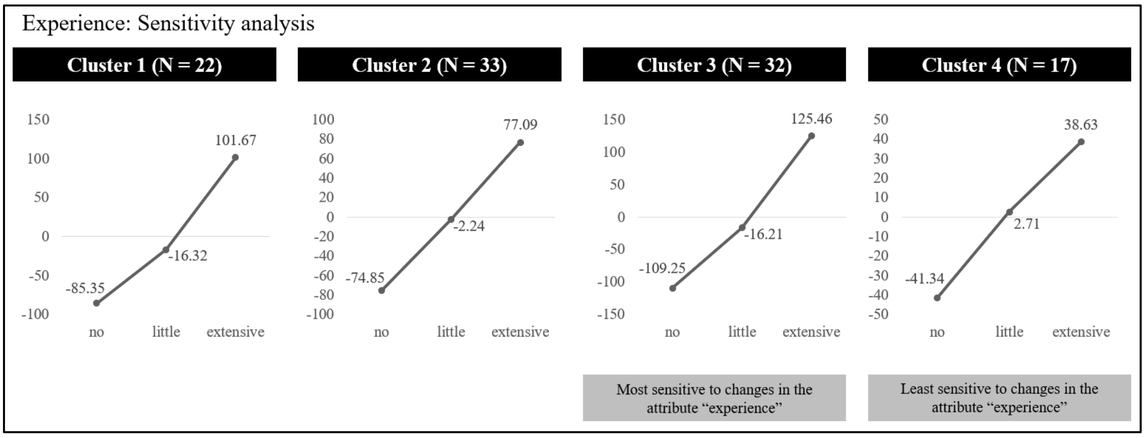
Notes: N = 104; Tukey-Kramer post-hoc tests were conducted to reveal statistically significant differences in the variable means of specific clusters; *** p<0.001, ** p<0.01, * p<0.05; [1]Measured on a 5-point Likert scale

A-3: Average utilities for the levels of the attribute “collaboration” per cluster



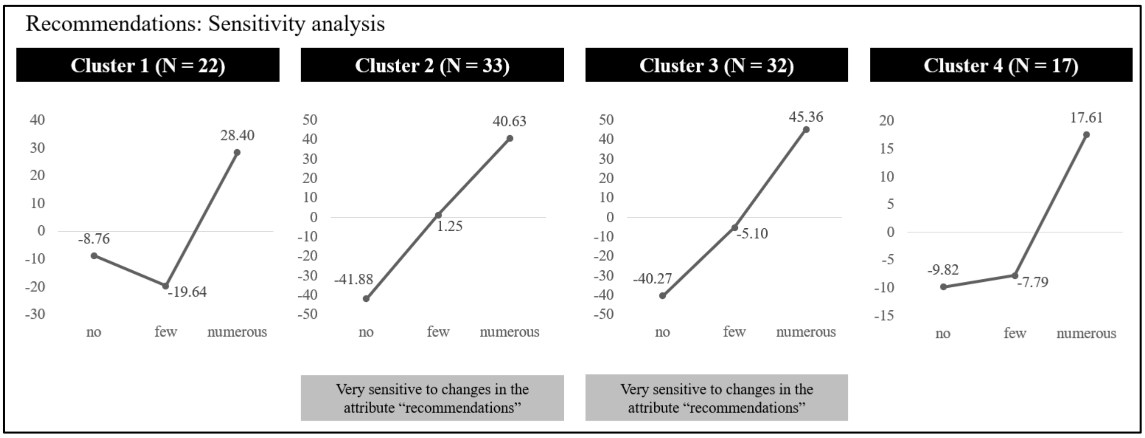
Notes: The figures displayed in the graphs are the utility estimates derived from an HB regression model.

A-4: Average utilities for the levels of the attribute “experience” per cluster



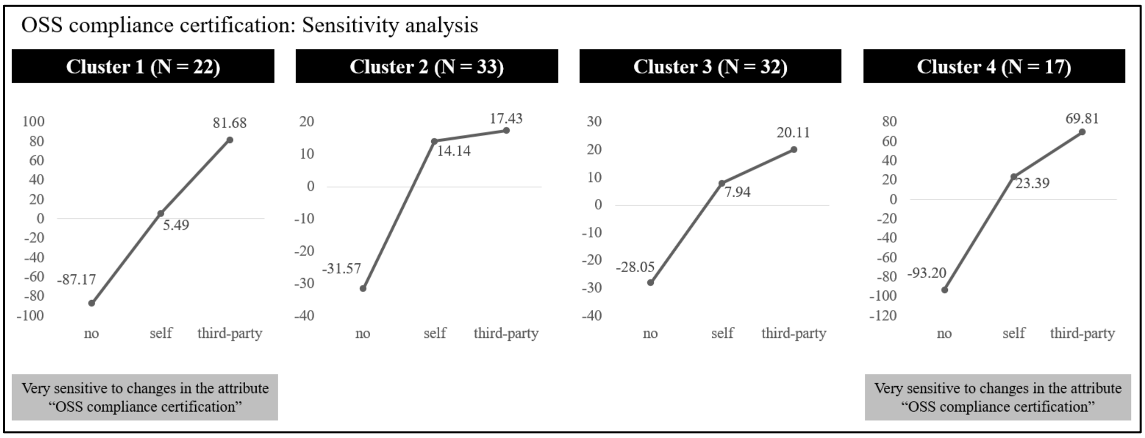
Notes: The figures displayed in the graphs are the utility estimates derived from an HB regression model.

A-5: Average utilities for the levels of the attribute “recommendations” per cluster



Notes: The figures displayed in the graphs are the utility estimates derived from an HB regression model.

A-6: Average utilities for the levels of the attribute “OSS compliance certification” per cluster



Notes: The figures displayed in the graphs are the utility estimates derived from an HB regression model.

References

Ågerfalk, P. J., & Fitzgerald, B. (2008). Outsourcing to an Unknown Workforce: Exploring Opensurcing as a Global Sourcing Strategy. *MIS Quarterly*, *32*(2), 385–409. https://doi.org/10.2307/25148845

Aguinis, H., Gottfredson, R. K., & Culpepper, S. A. (2013). Best-Practice Recommendations for Estimating Cross-Level Interaction Effects Using Multilevel Modeling. *Journal of Management*, *39*(6), 1490–1528. https://doi.org/10.1177/0149206313478188

Anderson, S. W., Daly, J. D., & Johnson, M. F. (1999). Why Firms Seek ISO 9000 Certification: Reglatory Compliance or Competitive Advantage? *Production and Operations Management*, *8*(1), 28–43. https://doi.org/10.1111/j.1937-5956.1999.tb00059.x

Angulo, A. M., & Gil, J. M. (2007). Risk Perception and Consumer Willingness to Pay for Certified Beef in Spain. *Food Quality and Preference*, *18*(8), 1106–1117. https://doi.org/10.1016/j.foodqual.2007.05.008

Benlian, A., & Hess, T. (2011). Opportunities and Risks of Software-as-a-Service: Findings From a Survey of IT Executives. *Decision Support Systems*, *52*(1), 232–246. https://doi.org/10.1016/j.dss.2011.07.007

Bhattacharya, S. (1980). Nondissipative Signaling Structures and Dividend Policy. *The Quarterly Journal of Economics*, *95*(1), 1–24. https://doi.org/10.2307/1885346

Biong, H. (2013). Choice of Subcontractor in Markets with Asymmetric Information: Reputation and Price Effects. *Journal of Business & Industrial Marketing*, *28*(1), 60–71. https://doi.org/10.1108/08858621311285723

Blohm, I., Bretschneider, U., Leimeister, J. M., & Krcmar, H. (2011). Does Collaboration Among Participants Lead to Better Ideas in IT-based Idea Competitions? An Empirical Investigation. *International Journal of Networking and Virtual Organisations*, *9*(2), 106–122.

Blombäck, A., & Axelsson, B. (2007). The Role of Corporate Brand Image in the Selection of New Subcontractors. *Journal of Business & Industrial Marketing*, *22*(6), 418–430. https://doi.org/10.1108/08858620710780181

Boiral, O. (2012). Iso Certificates as Organizational Degrees? Beyond the Rational Myths of the Certification Process. *Organization Studies*, *33*(5-6), 633–654. https://doi.org/10.1177/0170840612443622

Boyd, D. E., Sese, F. J., & Tillmanns, S. (2022). The Design of B2B Customer References: A Signaling Theory Perspective. *Journal of the Academy of Marketing Science*, 1–17. https://doi.org/10.1007/s11747-022-00902-6

Brach, S., Walsh, G., & Shaw, D. (2018). Sustainable Consumption and Third-Party Certification Labels: Consumers' Perceptions and Reactions. *European Management Journal*, *36*(2), 254–265. https://doi.org/10.1016/j.emj.2017.03.005

Brown, A., van der Wiele, T., & Loughton, K. (1998). Smaller Enterprises' Experiences with ISO 9000. *International Journal of Quality & Reliability Management*, *15*(3), 273–285. https://doi.org/10.1108/02656719810198935

Capra, E., Francalanci, C., Merlo, F., & Rossi Lamastra, C. (2009). A Survey on Firms' Participation in Open Source Community Projects. In C. Boldyreff, K. Crowston, B.

Lundell, & A. I. Wasserman (Eds.), *Open Source Ecosystems: Diverse Communities Interacting* (pp. 225–236). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-02032-2_20

Chengalur-Smith, I., Nevo, S., & Demertzoglou, P. (2010). An Empirical Analysis of the Business Value of Open Source Infrastructure Technologies. *Journal of the Association for Information Systems*, *11*(11), 708–729. https://doi.org/10.17705/1jais.00242

Chesbrough, H. W. (2003). *Open Innovation: The New Imperative for Creating and Profiting from Technology*. Harvard Business Press.

Chrzan, K. (1994). Three Kinds of Order Effects in Choice-Based Conjoint Analysis. *Marketing Letters*, *5*(2), 165–172. https://doi.org/10.1007/BF00994106

Chrzan, K. (2015). How Many Holdout Tasks for Model Validation? *Sawtooth Software Research Paper Series*. https://sawtoothsoftware.com/resources/technical-papers/how-many-holdout-tasks-for-model-validation

Chrzan, K., & Orme, B. (2000). An Overview and Comparison of Design Strategies for Choice-Based Conjoint Analysis. *Sawtooth Software Research Paper Series*, 161–178.

Comar, C., Gasperoni, F., & Ruiz, J. F. (2009). Open-DO: An Open-Source Initiative for the Development of Safety-Critical Software. In *4th IET International Conference on Systems Safety 2009. Incorporating the SaRS Annual Conference.* IET. https://doi.org/10.1049/cp.2009.1576

Connelly, B. L., Certo, S. T., & Ireland, R. D. (2011). Signaling Theory: A Review and Assessment. *Journal of Management*, *37*(1), 39–67. https://doi.org/10.1177/0149206310388419

Corbett, C. J., & Kirsch, D. A. (2001). International Diffusion of ISO 14000 Certification. *Production and Operations Management*, *10*(3), 327–342. https://doi.org/10.1111/j.1937-5956.2001.tb00378.x

Cronbach, L. J. (1951). Coefficient Alpha and the Internal Structure of Tests. *Psychometrika*, *16*(3), 297–334. https://doi.org/10.1007/BF02310555

Dahlander, L. (2007). Penguin in a new Suit: A Tale of how De Novo Entrants Emerged to Harness Free and Open Source Software Communities. *Industrial and Corporate Change*, *16*(5), 913–943. https://doi.org/10.1093/icc/dtm026

Dahlander, L., & Gann, D. M. (2010). How Open is Innovation? *Research Policy*, *39*(6), 699–709. https://doi.org/10.1016/j.respol.2010.01.013

Dahlander, L., & Magnusson, M. G. (2005). Relationships Between Open Source Software Companies and Communities: Observations from Nordic Firms. *Research Policy*, *34*(4), 481–493. https://doi.org/10.1016/j.respol.2005.02.003

Dahlander, L., & Magnusson, M. (2008). How do Firms Make Use of Open Source Communities? *Long Range Planning*, *41*(6), 629–649. https://doi.org/10.1016/j.lrp.2008.09.003

Daniel, S., Maruping, L., Cataldo, M [M.], & Herbsleb, J [J.] (2018). The Impact of Ideology Misfit on Open Source Software Communities and Companies. *Management Information Systems Quarterly*, *42*(4), 1069-1096. https://doi.org/10.25300/MISQ/2018/14242

Daniel, S., Midha, V., Bhattacherhjee, A., & Singh, S. P. (2018). Sourcing Knowledge in Open Source Software Projects: The Impacts of Internal and External Social Capital on Project Success. *The Journal of Strategic Information Systems*, *27*(3), 237–256. https://doi.org/10.1016/j.jsis.2018.04.002

Daniel, S. L., Maruping, L. M., Cataldo, M [Marcelo], & Herbsleb, J [Jim] (2018). The Impact of Ideology Misfit on Open Source Software Communities and Companies. *Management Information Systems Quarterly*, *42*(4). https://doi.org/10.25300/MISQ/2018/14242

Eaton, B., Elaluf-Calderwood, S., Sørensen, C., & Yoo, Y. (2015). Distributed Tuning of Boundary Resources: The Case of Apple's iOS Service System. *MIS Quarterly*, *39*(1), 217–243. https://www.jstor.org/stable/26628348

Everitt, B. S., Landau, S., Leese, M., & Stahl, D. (2011). *Cluster Analysis* (5th ed.). *Wiley series in probability and statistics*. Wiley.

Fabbrini, F., Fusani, M., & Marchetti, E. (2013). Process Scenarios in Open Source Software Certification. *Electronic Communications of the EASST*, *48*.

Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-Services Adoption: A Perceived Risk Facets Perspective. *International Journal of Human-Computer Studies*, *59*(4), 451–474. https://doi.org/10.1016/s1071-5819(03)00111-3

Feller, J., Finnegan, P., Fitzgerald, B., & Hayes, B. (2008). From Peer Production to Productization: A Study of Socially Enabled Business Exchanges in Open Source Service Networks. *Information Systems Research*, *19*(4), 475–493. https://doi.org/10.1287/isre.1080.0207

Feuser, J., & Peleska, J. (2010). Security in Open Model Software with Hardware Virtualisation – The Railway Control System Perspective. *Electronic Communications of the EASST*, *33*(0). https://doi.org/10.14279/tuj.eceasst.33.451

Flick, U. (2022). *An Introduction to Qualitative Research*. SAGE.

Forte, A., & Lampe, C. (2013). Defining, Understanding, and Supporting Open Collaboration. *American Behavioral Scientist*, *57*(5), 535–547. https://doi.org/10.1177/0002764212469362

Fusani, M., & Marchetti, E. (2010). Damages and Benefits of Certification: A Perspective From an Independent Assessment Body. *Electronic Communications of the EASST*, *33*(0). https://doi.org/10.14279/tuj.eceasst.33.450 (Electronic Communications of the EASST, Volume 33: Foundations and Techniques for Open Source Software Certification 2010).

Gangadharan, G. R., D’Andrea, V., Paoli, S. de, & Weiss, M. (2012). Managing License Compliance in Free and Open Source Software Development. *Information Systems Frontiers*, *14*(2), 143–154. https://doi.org/10.1007/s10796-009-9180-1

German, D., & Di Penta, M. (2012). A Method for Open Source License Compliance of Java Applications. *IEEE Software*, *29*(3), 58–63. https://doi.org/10.1109/ms.2012.50

Germonprez, M., Kendall, J. E., Kendall, K. E., Mathiassen, L., Young, B. W., & Warner, B. (2017). A Theory of Responsive Design: A Field Study of Corporate Engagement with Open Source Communities. *Information Systems Research*, *28*(1). https://doi.org/10.1287/isre.2016.0662

Germonprez, M., Young, B. W., Mathiassen, L., Kendall, J. E., & Kendall, K. E. (2012). Risk Mitigation in Corporate Participation with Open Source Communities: Protection and Compliance in an Open Source Supply Chain. *International Research Workshop on IT Project Management*. https://aisel.aisnet.org/irwitpm2012/3/

Ghazawneh, A., & Henfridsson, O. (2013). Balancing Platform Control and External Contribution in Third-Party Development: The Boundary Resources Model. *Information Systems Journal*, *23*(2), 173–192. https://doi.org/10.1111/j.1365-2575.2012.00406.x

Goebel, P., Reuter, C., Pibernik, R., Sichtmann, C., & Bals, L. (2018). Purchasing Managers' Willingness to Pay for Attributes that Constitute Sustainability. *Journal of Operations Management*, *62*(1), 44–58. https://doi.org/10.1016/j.jom.2018.08.002

Green, P. E., & Srinivasan, V. (1990). Conjoint Analysis in Marketing: New Developments with Implications for Research and Practice. *Journal of Marketing*, *54*(4), 3–19. https://doi.org/10.2307/1251756

Gregory, R. W., Kaganer, E., Henfridsson, O., & Ruch, T. (2018). IT Consumerization and the Transformation of IT Governance. *MIS Quarterly*, *42*(4), 1225–1253. https://misq.umn.edu/skin/frontend/default/misq/pdf/appendices/2018/v42i4appendices/10_13703_ra_gregorykaganerappendices.pdf

Haddad, I. (2016). *An Introduction to Open Source Compliance in the Enterprise*. https://www.linuxfoundation.org/blog/blog/an-introduction-to-open-source-compliance-in-the-enterprise

Hair, J. F., Anderson, R. E., Babin, B. J., & Black, W. C. (2010). *Multivariate Data Analysis: A Global Perspective* (7th ed.). Pearson. https://scholar.google.de/citations?user=jmvuqpsaaaaj&hl=de&oi=sra

Harutyunyan, N. (2020). Managing Your Open Source Supply Chain - Why and How? *Computer*, *53*(6), 77–81. https://doi.org/10.1109/mc.2020.2983530

Helm, R., & Mark, A. (2007). Implications from Cue Utilization Theory and Signalling Theory for Firm Reputation and the Marketing of New Products. *International Journal of Product Development*, *4*(3/4), 396-411. https://www.researchgate.net/profile/roland-helm/publication/5140838_implications_from_cue_utilization_theory_and_signalling_theory_for_firm_reputation_and_the_marketing_of_new_products

Helm, S., & Salminen, R. T. (2010). Basking in Reflected Glory: Using Customer Reference Relationships to Build Reputation in Industrial Markets. *Industrial Marketing Management*, *39*(5), 737–743. https://doi.org/10.1016/j.indmarman.2010.02.012

Helms, E., & Williams, L. (2011). Evaluating Access Control of Open Source Electronic Health Record Systems. In *Proceedings of the 3rd Workshop on Software Engineering in Health Care.* ACM. https://doi.org/10.1145/1987993.1988006

Ho, C.-T., & Wei, C.-L. (2016). Effects of Outsourced Service Providers' Experiences on Perceived Service Quality: A Signaling Theory Framework. *Industrial Management & Data Systems*, *116*(8), 1656–1677. https://doi.org/10.1108/IMDS-01-2016-0015

Ho, S. Y., & Rai, A. (2017). Continued Voluntary Participation Intention in Firm-Participating Open Source Software Projects. *Information Systems Research*, *28*(3), 603–625. https://doi.org/10.1287/isre.2016.0687

Howison, J., & Crowston, K [Kevin] (2014). Collaboration Through Open Superposition: A Theory of the Open Source Way. *MIS Quarterly*, *38*(1), 29–50. https://doi.org/10.25300/misq/2014/38.1.02

Hui, K.-L., Teo, H.-H., & Lee, S.-Y. T. (2007). The Value of Privacy Assurance: An Exploratory Field Experiment. *MIS Quarterly*, *31*(1), 19. https://doi.org/10.2307/25148779

International Organization for Standardization. (1996). *ISO/IEC Guide 2: Standardization and related activities - General vocabulary.*

Irwin. (1996). *ISO 9000 Survey*. Burr Ridge, U.S.

Johnson, R., & Orme, B. (1996). How Many Questions Should You Ask in Choice-Based Conjoint Studies? *Sawtooth Software Research Paper Series*. https://www.sawtoothsoftware.com/download/techpap/howmanyq.pdf

Johnston, W. J., & Lewin, J. E. (1996). Organizational Buying Behavior: Toward an Integrative Framework. *Journal of Business Research*, *35*(1), 1–15. https://doi.org/10.1016/0148-2963(94)00077-8

Kaas, K. P. (1991). Marktinformationen: Screening und Signaling unter Partnern und Rivalen. *Zeitschrift Für Betriebswirtschaftslehre*, *61*(3), 357–370.

Kakarontzas, G., Katsaros, P., & Stamelos, I. (2010). Component Certification as a Prerequisite forWidespread OSS Reuse. *Electronic Communications of the EASST*, *33*(0). https://doi.org/10.14279/tuj.eceasst.33.449

Kalliamvakou, E., Weber, J., & Knauss, A. (2016). Certification of Open Source Software – A Scoping Review. In *12th IFIP International Conference on Open Source Systems Proceedings* (pp. 111–122). Springer, Cham. https://doi.org/10.1007/978-3-319-39225-7_9

Kaplan, S. E., & Nieschwietz, R. J. (2003). A Web Assurance Services Model of Trust for B2C e-Commerce. *International Journal of Accounting Information Systems*, *4*(2), 95–114. https://doi.org/10.1016/s1467-0895(03)00005-8

Ke, W., & Zhang, P. (2010). The Effects of Extrinsic Motivations and Satisfaction in Open Source Software Development. *Journal of the Association for Information Systems*, *11*(12), 784-808. https://doi.org/10.17705/1jais.00251

Ketchen, D. J., & Shook, C. L. (1996). The Application of Cluster Analysis in Strategic Management Research: An Analysis and Critique. *Strategic Management Journal*, *17*(6), 441–458. https://doi.org/10.1002/(SICI)1097-0266(199606)17:6<441::AID-SMJ819>3.0.CO;2-G

Khoroshilov, A. (2009). Open Source Certification and Educational Process. *Electronic Communications of the EASST, 20.* https://doi.org/10.14279/tuj.eceasst.20.255 (Electronic Communications of the EASST, Volume 20: Foundations and Techniques for Open Source Certification 2009).

King, J. T [Jason Tyler], Smith, B., & Williams, L. (2012). Modifying Without a Trace: General Audit Guidelines are Inadequate for Open-Source Electronic Health Record Audit Mechanisms. In *Proceedings of the 2nd ACM SIGHIT International Health Informatics Symposium.* ACM. https://doi.org/10.1145/2110363.2110399

Kirmani, A., & Rao, A. R. (2000). No Pain, No Gain: A Critical Review of the Literature on Signaling Unobservable Product Quality. *Journal of Marketing*, *64*(2), 66–79. https://doi.org/10.1509/jmkg.64.2.66.18000

Koltun, P. (2011). Free and Open Source Software Compliance: An Operational Perspective. *International Free and Open Source Software Law Review*, *3*(1), 95-101. https://doi.org/10.5033/ifosslr.v3i1.61

Kotler, P., & Pfoertsch, W. (2007). Being Nnown or Being One of Many: The Need for Brand Management for Business-to-Business (B2B) Companies. *Journal of Business & Industrial Marketing*, *22*(6), 357–362. https://doi.org/10.1108/08858620710780118

Krogh, G. von, Haefliger, S., Spaeth, S., & Wallin, M. W. (2012). Carrots and Rainbows: Motivation and Social Practice in Open Source Software Development. *MIS Quarterly*, *36*(2), 649–676. https://doi.org/10.2307/41703471

Krogh, G. von, Spaeth, S., & Lakhani, K. R. (2003). Community, Joining, and Specialization in Open Source Software Innovation: A Case Study. *Research Policy*, *32*(7), 1217–1241. https://doi.org/10.1016/s0048-7333(03)00050-7

Lakhani, K. R., & Wolf, R. G. (2003). Why Hackers Do What They Do: Understanding Motivation and Effort in Free/Open Source Software Projects. *SSRN Journal*. Advance online publication. https://doi.org/10.2139/ssrn.443040

Lang, M., Wiesche, M., & Krcmar, H. (2018). Criteria for Selecting Cloud Service Providers: A Delphi Study of Quality-of-Service Attributes. *Information & Management*, *55*(6), 746-758, https://doi.org 10.1016/j.im.2018.03.004

Lee, J., Park, H., & Zaggl, M. A. (2022). When to Signal? Contingencies for Career-Motivated Contributions in Online Collaboration Communities. *Journal of the Association for Information Systems*, *23*(6), 1386–1419. https://doi.org/10.17705/1jais.00765

Lee, T. Y. (1998). The Development of ISO 9000 Certification and the Future of Quality Management: A Survey of Certified Firms in Hong Kong. *International Journal of Quality & Reliability Management*, *15*(2), 162–177. https://doi.org/10.1108/02656719810204766

Leimeister, J. M., Huber, M., & Bretschneider, U. (2009). Leveraging Crowdsourcing: Activation-Supporting Components for IT-Based Ideas Competition. *Journal of Management Information Systems*, *26*(1), 197–224. https://doi.org/10.2753/MIS0742-1222260108

Lenk, P. J., DeSarbo, W. S., Green, P. E., & Young, M. R. (1996). Hierarchical Bayes Conjoint Analysis: Recovery of Partworth Heterogeneity from Reduced Experimental Designs. *Marketing Science*, *15*(2), 173–191. https://doi.org/10.1287/mksc.15.2.173

Lindberg, A., Berente, N., Gaskin, J., & Lyytinen, K. (2016). Coordinating Interdependencies in Online Communities: A Study of an Open Source Software Project. *Information Systems Research*, *24*(4), 751–772. https://doi.org/10.1287/isre.2016.0673

Lins, S., & Sunyaev, A. (2017). Unblackboxing IT Certifications: A Theoretical Model Explaining IT Certification Effectiveness. *Thirty Eighth International Conference on Information Systems (ICIS 2017)*. https://www.researchgate.net/profile/sebastian-lins-2/publication/320014964_unblackboxing_it_certifications_a_theoretical_model_explaining_it_certification_effectiveness_short_paper

The Linux Foundation. (2022). *OpenChain Project*. https://www.openchainproject.org/

Louviere, J. J., & Woodworth, G. (1983). Design and Analysis of Simulated Consumer Choice or Allocation Experiments: An Approach Based on Aggregate Data. *Journal of Marketing Research*, *20*(4), 350. https://doi.org/10.2307/3151440

Macredie, R. D., & Mijinyawa, K. (2011). A Theory-Grounded Framework of Open Source Software Adoption in SMEs. *European Journal of Information Systems, 20*(2), 237–250. https://doi.org/10.1057/ejis.2010.60

Markus, M. L. (2007). The Governance of Free/Open Source Software Projects: Monolithic, Multidimensional, or Configurational? *Journal of Management & Governance*, *11*(2), 151–163. https://doi.org/10.1007/s10997-007-9021-x

Mauldin, E., & Arunachalam, V. (2002). An Experimental Examination of Alternative Forms of Web Assurance for Business-to-Consumer e-Commerce. *Journal of Information Systems*, *16*(s-1), 33–54. https://doi.org/10.2308/jis.2002.16.s-1.33

McGhee, D. D. (2007). Free and Open Source Software Licenses: Benefits, Risks, and Steps Toward Ensuring Compliance. *Intellectual Property & Technology Law Journal*, *19*(11), 5–9.

Medappa, P. K., & Srivastava, S. C. (2020). Ideological Shifts in Open Source Orchestration: Examining the Influence of Licence Choice and Organisational Participation on Open Source Project Outcomes. *European Journal of Information Systems, 29*, 500–520. https://doi.org/10.1080/0960085X.2020.1756003

Mehra, A., Dewan, R., & Freimer, M. (2011). Firms as Incubators of Open-Source Software. *Information Systems Research*, *22*(1), 22–38. https://doi.org/10.1287/isre.1090.0276

Michell, V., & Fitzgerald, B. (1997). The IT Outsourcing Market-Place: Vendors and Their Selection. *Journal of Information Technology*, *12*(3), 223–237. https://doi.org/10.1080/026839697345080

Milligan, G. W. (1980). An Examination of the Effect of Six Types of Error Perturbation on Fifteen Clustering Algorithms. *Psychometrika*, *45*(3), 325–342. https://doi.org/10.1007/BF02293907

Milligan, G. W., & Cooper, M. C. (1985). An Examination of Procedures for Determining the Number of Clusters in a Data Set. *Psychometrika*, *50*(2), 159–179. https://doi.org/10.1007/BF02294245

Mockus, A., Fielding, R. T., & Herbsleb, J [Jim] (2002). Two Case Studies of Open Source Software Development. *ACM Transactions on Software Engineering and Methodology (TOSEM)*, *11*(3), 309–346. https://doi.org/10.1145/567793.567795

Monroe, K. B., & Dodds, W. B. (1988). A Research Program for Establishing the Validity of the Price-Quality Relationship. *Journal of the Academy of Marketing Science*, *16*(1), 151–168. https://doi.org/10.1007/BF02723333

Morasca, S., Taibi, D., & Tosi, D. (2009). Towards Certifying the Testing Process of Open-Source Software: New Challenges or Old Methodologies? In *2009 ICSE Workshop on Emerging Trends in Free/Libre/Open Source Software Research and Development.* IEEE. https://doi.org/10.1109/floss.2009.5071356

Morgan, L., Feller, J., & Finnegan, P. (2013). Exploring Value Networks: Theorising the Creation and Capture of Value with Open Source Software. *European Journal of Information Systems*, *22*(5), 569–588. https://doi.org/10.1057/ejis.2012.44

Moyses-Scheingruber, S. (2020). Decision Criteria in Acquisition Target Screening: Decision Weights, Acquirer Types and Differences between Family and Non-Family Firms and within the Group of Family Firms. *Dissertation at University of Trier, Germany.* https://doi.org/10.25353/ubtr-xxxx-109e-55ca

Nöteberg, A., Christiaanse, E., & Wallage, P. (2003). Consumer Trust in Electronic Channels: The Impact of Electronic Commerce Assurance on Consumers' Purchasing Likelihood and Risk Perceptions. *E-Service Journal*, *2*(2), 46–67. https://doi.org/10.2979/esj.2003.2.2.46

O'Mahony, S. (2007). The Governance of Open Source Initiatives: What Does it Mean to be Community Managed? *Journal of Management & Governance*, *11*(2), 139–150. https://doi.org/10.1007/s10997-007-9024-7

O'Mahony, S., & Bechky, B. (2008). Boundary Organizations: Enabling Collaboration Among Unexpected Allies. *Administrative Science Quarterly*, *53*(3), 422–459. https://doi.org/10.2189/asqu.53.3.422

O'Mahony, S., & Ferraro, F. (2007). The Emergence of Governance in an Open Source Community. *Academy of Management Journal*, *50*(5), 1079–1106. https://doi.org/10.5465/amj.2007.27169153

Pekovic, S. (2010). The Determinants of ISO 9000 Certification: A Comparison of the Manufacturing and Service Sectors. *Journal of Economic Issues*, *44*(4), 895–914. https://doi.org/10.2753/JEI0021-3624440403

Plank, R. E., & Ferrin, B. G. (2002). How Manufacturers Value Purchase Offerings: An Exploratory Study. *Industrial Marketing Management*, *31*(5), 457–465.

Quirós, J. T., & Justino, M. d. R. F. (2013). A Comparative Analysis Between Certified and Non-Certified Companies Through the Quality Management System. *International Journal of Quality & Reliability Management*, *30*(9), 958–969. https://doi.org/10.1108/IJQRM-04-2011-0059

Rabe-Hesketh, S., & Everitt, B. (2003). *Handbook of Statistical Analyses Using Stata*. CRC Press.

Rajalahti, T., & Kvalheim, O. M. (2011). Multivariate Data Analysis in Pharmaceutics: A Tutorial Review. *International Journal of Pharmaceutics*, *417*(1-2), 280–290. https://doi.org/10.1016/j.ijpharm.2011.02.019

Rao, A. R., & Monroe, K. B. (1996). Causes and Consequences of Price Premiums. *The Journal of Business*, *69*(4), 511–535. https://doi.org/10.1086/209703

Rao, A. R., Qu, L., & Ruekert, R. W. (1999). Signaling Unobservable Product Quality Through a Brand Ally. *Journal of Marketing Research*, *36*(2), 258–268. https://doi.org/10.1177/002224379903600209

Riehle, D., & Harutyunyan, N. (2019). Open-Source License Compliance in Software Supply Chains. In *Towards Engineering Free/Libre Open Source Software (FLOSS) Ecosystems for Impact and Sustainability* (pp. 83–95). Springer, Singapore. https://doi.org/10.1007/978-981-13-7099-1_5

Riley, J. G. (2001). Silver Signals: Twenty-Five Years of Screening and Signaling. *Journal of Economic Literature*, *39*(2), 432–478. https://doi.org/10.1257/jel.39.2.432

Rolandsson, B., Bergquist, M., & Ljungberg, J. (2011). Open Source in the Firm: Opening up Professional Practices of Software Development. *Research Policy*, *40*(4), 576–587. https://doi.org/10.1016/j.respol.2010.11.003

Sabherwal, R., & King, W. R. (1995). An Empirical Taxonomy of the Decision-Making Processes Concerning Strategic Applications of Information Systems. *Journal of Management Information Systems*, *11*(4), 177–214. https://doi.org/10.1080/07421222.1995.11518064

Salminen, R. T., & Möller, K. (2006). Role of References in Business Marketing–Towards a Normative Theory of Referencing. *Journal of Business-to-Business Marketing*, *13*(1), 1–51. https://doi.org/10.1300/J033v13n01_01

Shah, S. K. (2006). Motivation, Governance, and the Viability of Hybrid Forms in Open Source Software Development. *Management Science*, *52*(7), 1000–1014. https://doi.org/10.1287/mnsc.1060.0553

Shapiro, C. (1982). Consumer Information, Product Quality, and Seller Reputation. *The Bell Journal of Economics*, *13*(1). https://doi.org/10.2307/3003427

Shepherd, D. A. (1999). Venture Capitalists' Assessment of New Venture Survival. *Management Science*, *45*(5), 621–632. https://doi.org/10.1287/mnsc.45.5.621

Shepherd, D. A., & Zacharakis, A. (Eds.). (2018). *Reflections and Extensions on Key Papers of the First Twenty-Five Years of Advances*. Emerald Publishing Limited.

Smith, B., Austin, A., Brown, M., King, J. T [Jason T.], Lankford, J., Meneely, A., & Williams, L. (2010). Challenges for Protecting the Privacy of Health Information. In *Proceedings of the Second Annual Workshop on Security and Privacy in Medical and Home-Care Systems.* ACM. https://doi.org/10.1145/1866914.1866916

Spaeth, S., Krogh, G. von, & He, F. (2015). Perceived Firm Attributes and Intrinsic Motivation in Sponsored Open Source Software Projects. *Information Systems Research*, *26*(1), 224–237. https://doi.org/10.1287/isre.2014.0539

Spence, M. (1973). Job Market Signaling. *The Quarterly Journal of Economics*, *87*(3), 355–374. https://doi.org/10.2307/1882010

Spence, M. (1974). Competitive and Optimal Responses to Signals: An Analysis of Efficiency and Distribution. *Journal of Economic Theory*, *7*(3), 296–332. https://doi.org/10.1016/0022-0531(74)90098-2

Spence, M. (2002). Signaling in Retrospect and the Informational Structure of Markets. *American Economic Review*, *92*(3), 434–459. https://doi.org/10.1257/00028280260136200

Stewart, K. J., Ammeter, A. P., & Maruping, L. M. (2006). Impacts of License Choice and Organizational Sponsorship on User Interest and Development Activity in Open Source Software Projects. *Information Systems Research*, *17*(2), 126–144. https://doi.org/10.1287/isre.1060.0082

Strauss, A. L. (1987). *Qualitative Analysis for Social Scientists*. Cambridge University Press.

Svahn, F., Mathiassen, L., & Lindgren, R. (2017). Embracing Digital Innovation in Incumbent Firms: How Volvo Cars Managed Competing Concerns. *MIS Quarterly*, *41*(1), 239–254. https://www.jstor.org/stable/26629645

Terziovski, M., Samson, D., & Dow, D. (1997). The Business Value of Quality Management Systems Certification. Evidence from Australia and New Zealand. *Journal of Operations Management*, *15*(1), 1–18. https://doi.org/10.1016/s0272-6963(96)00103-9

Tirole, J. (1988). *The Theory of Industrial Organization*. MIT Press.

Tukey, J. W. (1949). Comparing Individual Means in the Analysis of Variance. *Biometrics*, *5*(2), 99–114. https://doi.org/10.2307/3001913

Välimäki, M. (2005). How to Manage IPR Infringement Risks in Open Source Development. In WSOY (Ed.), *Intellectual Property Beyond Rights* (pp. 347–364). WSOY.

van der Pijl, G. J., Swinkels, G., & Verrijdt, J. G. (1997). Iso 9000 versus CMM: Standardization and Certification of IS Development. *Information & Management*, *32*(6), 267–274. https://doi.org/10.1016/s0378-7206(97)00019-0

Wareham, J., Fox, P., & Cano Giner, J. L. (2014). Technology Ecosystem Governance. *Organization Science*, *25*(4), 1195–1215. https://doi.org/10.1287/orsc.2014.0895

Wathne, K. H., Biong, H., & Heide, J. B. (2001). Choice of Supplier in Embedded Markets: Relationship and Marketing Program Effects. *Journal of Marketing*, *65*(2), 54–66. https://doi.org/10.1509/jmkg.65.2.54.18254

West, J., & Gallagher, S. (2006). Challenges of Open Innovation: The Paradox of Firm Investment in Open-Source Software. *R&D Management*, *36*(3), 319–331. https://doi.org/10.1111/j.1467-9310.2006.00436.x

Wu, J., & Gaytán, E. A. A. (2013). The Role of Online Seller Reviews and Product Price on Buyers' Willingness-to-Pay: A Risk Perspective. *European Journal of Information Systems*, *22*(4), 416–433. https://doi.org/10.1057/ejis.2012.33

Wuyts, S., Verhoef, P. C., & Prins, R. (2009). Partner Selection in B2B Information Service Markets. *International Journal of Research in Marketing*, *26*(1), 41–51. https://doi.org/10.1016/j.ijresmar.2008.07.008

Yin, R. K. (2009). *Case Study Research: Design and Methods*. SAGE.

Yun, H. Y., Joe, Y. J., & Shin, D. M. (2017). Method of License Compliance of Open Source Software Governance. In *8th IEEE International Conference on Software Engineering and Service Science (ICSESS)* (pp. 83–86). IEEE. https://doi.org/10.1109/icsess.2017.8342869

Zacharakis, A., & Meyer, G. D. (2000). The Potential of Actuarial Decision Models: Can They Improve the Venture Capital Investment Decision? *Journal of Business Venturing, 15*, 323–346.

Zaggl, M. A., Malhotra, A., Alexy, O., & Majchrzak, A. (2023). Governing Crowdsourcing for Unconstrained Innovation Problems. *Strategic Management Journal*, *35*(1). https://doi.org/10.1002/smj.3505