Journal Pre-proof

Software Compliance Requirements, Factors, and Policies: a Systematic Literature Review

Mohammed Mubarkoot , Jörn Altmann , Morteza Rasti-Barzoki , Bernhard Egger , Hyejin Lee

PII: S0167-4048(22)00377-7
DOI: https://doi.org/10.1016/j.cose.2022.102985
Reference: COSE 102985

To appear in: *Computers & Security*

Received date: 7 July 2022
Revised date: 3 October 2022
Accepted date: 21 October 2022

Please cite this article as: Mohammed Mubarkoot , Jörn Altmann , Morteza Rasti-Barzoki , Bernhard Egger , Hyejin Lee , Software Compliance Requirements, Factors, and Policies: a Systematic Literature Review, *Computers & Security* (2022), doi: https://doi.org/10.1016/j.cose.2022.102985

This is a PDF file of an article that has undergone enhancements after acceptance, such as the addition of a cover page and metadata, and formatting for readability, but it is not yet the definitive version of record. This version will undergo additional copyediting, typesetting and review before it is published in its final form, but we are providing this version to give early visibility of the article. Please note that, during the production process, errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

© 2022 The Author(s). Published by Elsevier Ltd.
This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/)

Journal Pre-proof

Software Compliance Requirements, Factors, and Policies:
a Systematic Literature Review

Mohammed Mubarkoot[a], Jörn Altmann[a,b], Morteza Rasti-Barzoki[c], Bernhard Egger[d], Hyejin Lee[a]

a. Technology Management Economics and Policy Program, College of Engineering, Seoul National University, 08826 Seoul, South Korea

b. Institute of Engineering Research, College of Engineering, Seoul National University, 08826 Seoul, South Korea

c. Department of Industrial and Systems Engineering, Isfahan University of Technology, Isfahan 84156-83111, Iran

d. Department of Computer Science and Engineering, College of Engineering, Seoul National University, 08826 Seoul, South Korea

mubarkoot@snu.ac.kr, jorn.altmann@acm.org, rasti@cc.iut.ac.ir, bernhard@csap.snu.ac.kr, hjhjinlee@snu.ac.kr

Abstract

Background:
Recent statistics reveal that 56% of software attacks are caused by insider negligence and 26% are caused by malicious insiders. They also show that 67% of organizations experience at least 21 incidents per year. Most of these incidents require significant time and effort to contain them. In this regard, ensuring compliance with corporate policies, regulations, and industry best practices is paramount.
Purpose: This study investigates software compliance requirements, factors, and policies together with the challenges they address. By taking a wider perspective, this study aims at bringing an understanding of existing research foci, evolving issues, and research directions.
Method: The study uses a systematic literature review and keyword analysis, to identify relevant studies that address the derived research questions. Considering scholarly articles published in the last decade, 4,772 results were retrieved and checked through an initial screening. A thorough screening is then conducted to further reduce the results to 77 primary articles.
Findings: The requirement on security of end users is gaining more attention. There is an emphasis on the gap between domain and compliance experts on the one side and software engineers on the other side. The review also identified 55 factors (and their underlying theories) that impact behavioral compliance with a majority of them focusing on individuals. Our results also list nineteen policies and compliance challenges they address. No distinction is found between open-source and proprietary software among the reviewed studies. The most mentioned policies are security education, training, and awareness (SETA), compliance automation, and organizational climate. The evolving topics in the field are: theory of workarounds, compliance and privacy by design, policy as code, security stress, and home-office users.
Implications: The review provides 9 recommendations, comprising practical implications for decision makers, theoretical implications for future research, and potential enhancement of the underlying theories.

Keywords: Software Compliance, Requirements, Policies, Factors, Impact, Systematic literature Review

1. Introduction

People count on the reliability of software services, as they need to trust critical infrastructure and complex software solutions [1]. Software disruptions and downtimes cause a significant financial burden to businesses. A 2016 study by the Ponemon Institute shows that the mean cost of a data center outage is close to $650,000 [2], let alone reputation and other consequences resulting from such downtimes. Malicious, non malicious, negligent and compromised users are considered a serious and growing risk, in that credential theft costs have increased 65% in the last two years, taking huge time and effort to contain

Journal Pre-proof

them [3]. Such challenges can be viewed from both a technological and a human side. While technology requires continuous monitoring and maintenance to ensure compliance, the human side is considered the weakest link in the compliance chains [4]. In fact, studies consistently reported that employees are responsible for over 50% of security breaches [5]-[6]. PricewaterhouseCoopers [7] reported that recovery from security breaches can take an average of 19 hours; the report revealed that more than 28% of businesses have no idea about how many attacks they experienced. The report also shows that 48% of employees lack security awareness and training programs, and 54% of employees reported an absence of a clear incident response process [7].

Software systems are precious assets to organizations, and ensuring compliance with various requirements, industry standards, and best practices is a top challenge. The multifaceted set of compliance sources complicates compliance management. This can be viewed from a perspective of the highly dynamic nature of technology and related laws that govern the evolution of software on the one hand [8], and the evolving compliance sources (i.e., regulations, policies, security requirements, best practices) [9] on the other hand. Technological approaches are not sufficient in securing information systems in organizations. Studies show that end users generally do not take appropriate actions as prescribed in the information security policies [10]-[11]. Similarly, developers also lack a sense of responsibility to deliver beyond just functionality (e.g., implementing privacy by design). While software systems can be either developed in-house, outsourced to a third party, deployed as a third-party commercial off the shelf, or provided as cloud-based services [12], it is of highly important to shed the light on requirements, factors, and policies of software compliance. The aim of this review is to provide an understanding on existing research focus, evolving topics and potential research directions on software compliance requirements, impacting factors and policies needed.

Existing reviews focus primarily on a certain industry or a specific aspect of compliance. No prior review work investigated the state-of-the-art compliance requirements, factors, and policies that impact different aspects in software compliance in a wider perspective. The relevance of this study comes from the growing concerns for software and information security and insider threats, in addition to the diversity of compliance sources and requirements. In this regard, bringing an understanding on existing research focuses and on evolving issues and directions is worth investigating.

In detail, this review aims at answering three research questions, which have been formulated and confirmed by analyzing existing review literature [5], [8], [9], [13]–[18]. The result of the analysis, which is shown in Table 1, depicts the lack of research on software compliance requirements, software compliance factors, and policies. The research questions are:

- **RQ1:** What are the software compliance requirements with respect to different industries and user contexts? (Section 4.2);
- **RQ2:** What are the factors that impact software compliance and which aspects of compliance are impacted? (Section 4.3);
- **RQ3:** What are the existing software compliance policies and which compliance challenges do they tend to address? (Section 4.4)

A systematic literature review (SLR) of Kitchenham et al. [19] is adapted to collect evidence for answering the research questions. The SLR is selected as an appropriate method for conducting this research, because it provides an explicit and replicable way for identifying and synthesizing the existing body of knowledge while minimizing bias and information overload. Furthermore, the aforementioned method is considered more suitable for reviewing software related research. For this, we systematically searched the scholarly databases to retrieve relevant research articles. In parallel, an initial screening is

Journal Pre-proof

conducted as a first level of eliminating irrelevant articles, reducing the number of articles to 484. Followed by a thorough screening and applying a set of criteria for inclusion and exclusion, 77 most relevant and influential articles have been identified.

Studying these 77 primary articles, 14 compliance requirements were identified. Among these, security and legal issues are highly discussed in the context of end users and software engineers. Furthermore, 19 policies were found and, based on them, compliance challenges that the policies address were listed. The results showed that, since most compliance violations and security breaches happen due to human behavior, security awareness is found critical to addressing many compliance challenges. Other highly discussed policies are automated management of compliance, enhancement of organizational climate, as well as development of deterrence instruments. The review also identified 55 factors that have an impact on different aspects of information systems policies compliance. The majority of these factors focus on individual aspects followed by organizational and cultural aspects. The study further delivers theoretical and practical implications, and proposes directions for potential areas for research.

The remainder of this paper is structured as follows: Section 2 provides an overview of related review papers and discusses them. Section 3 describes the methodology and the review process. Section 4 discusses the analysis of results and corresponding research questions. Section 5 elaborates on key highlights of the review and presents implications. Section 6 summarizes the key highlights, limitations and future directions.

2. Related Work on Software Compliance

Several review articles related to the research objective have been identified. Their studies focus primarily on a certain industry or a specific aspect of compliance. Based on their research focus, we summarize them into five categories: information security (IS), theoretical foundation of IS, insiders' behavior, factors in a specific industry, and bring your own device (BYOD). The common denominator among these reviews is security compliance and human subject. The human subject is considered more complicated than technological ones [4], more attention is paid to studying issues related to human behavior. Therefore, the focus of these categories in review literature represents the importance of these topics in the field of software compliance.

2.1. Information Security

Cram et al. [8] investigated organizational information security policies and synthesized a framework consisting of five sets of relationships. These relationships focus on the design and implementation of policies, the influence of security policies on the organization and employees, the influence of the organization and individual factors on policy compliance, the impact of policy compliance on organizational objectives, and changes of policy design. Another study by Balozian and Leidner [5] focuses on compliance of insiders with information systems' policies. They developed four themes to establish the building blocks of an indigenous information systems security theory. These themes consist of a philosophy of information security management, procedural countermeasures, technical countermeasures, and environmental countermeasures.

2.2. Theoretical Foundation for Information Security

Other review works pay more attention to applications of theories in the field of information systems

Journal Pre-proof

security compliance. Trang and Brendel [9] examine the applicability of deterrence theory in information security policy compliance research. They conclude that sanctions have an overall impact on deviant behavior in information security policy, and deterrence theory provides a better prediction of deviant behavior in malicious contexts, cultures with a high degree of power distance, and cultures with a high uncertainty avoidance. Prior to that, D'Arcy and Herath [14] attempted to study the discrepant findings in the information systems (IS) deterrence literature. Their study clarifies that scientific knowledge about deterrence theory in the IS security realm remains incomplete. They also show inconsistency and, in some cases, contradictory findings of deterrence theory in IS security, concluding that policies and procedures can be guided more by faith than facts.

2.3. Information Security Insider Behavior

Ali et al. [13] investigate information security policy compliance and information security behavior, aiming at identifying the behavioral transformation process from noncompliance to compliance. They find that there is more focus on compliance behaviors than noncompliance behaviors. Their study also finds that value conflicts, security-related stress, and neutralization are significant towards noncompliance, while internal/external and protection motivations have a positive and significant effect towards compliance behaviors. Ali et al. [13] conclude that deterrence techniques, management behaviors, culture, and information security awareness, play a vital role in transforming employees' behavior from noncompliance to compliance. Similarly, Tsohou and Holtkamp [17] survey the competencies associated with users' information security policy compliance behavior. Their study identifies a set of competencies associated with information security policy compliance and provides evidence on the lack of attention in information security responsibilities.

2.4. Compliance Factors in Specific Industries

Another set of review articles focuses only on a certain industry or on a specific context. Zandesh et al. [18] study the factors of a proper legal framework for healthcare systems in the cloud. Their study developed a framework that should be considered by the healthcare industry before transitioning to the cloud. The framework consists of five pillars, these are: compliance, data protection, identity credential access management, ownership, and quality of service. Similarly, but in different sectors, Hina and Dominic [15] study information security policies' compliance in higher education institutions. They develop insight from theories and a set of factors that significantly contribute to information security policy compliance. Their study concluded that awareness of information security policy compliance and follow-up procedures is the first and foremost step in achieving better information systems security. They also find that end users are usually unaware of response efficacy and therefore remain victims of malicious attacks most of the time. Hina and Dominic [15] argue that employees in higher education institutions are the least concerned, motivated, and aware of the potential threats that can harm their personal and work computing environment.

2.5. Bring Your Own Device (BYOD)

Finally, to assess compliance challenges and security risks associated with bring-your-own-device (BYOD) policies to workplaces, Palanisamy et al. [16] investigate security risks, challenges posed by employees' security policy noncompliance behavior and strategies to mitigate risks resulting from BYOD. The study found that there is a lack of focus on social factors within organizations on such policies. Moreover, the social surroundings can influence employees' decisions with security compliance

Journal Pre-proof

behavior. Palanisamy et al. [16] also conclude that there is a lack of research on security policy compliance and policy effectiveness in BYOD.

2.6. Comparison

While existing review papers address a specific aspect of compliance such as security policy or insiders' behavior; or focus on a certain context or theories (Table.1), no prior review investigated the state-of-the-art literature on software compliance and examines requirements, policies, and factors and their impact on different facets of compliance regardless of the context or industry.

Table.1. Summary of existing review studies

Study	Focus	Compliance Requirements	Specific Requirement on Information Security	Specific Industry	Theory	Factors	Policies
Cram et al. [8]	Organizational IS		✓				
Balozian & Leidner [5]	Indigenous IS security theory (Insider behavior)				✓	✓	
Trang and Brendel [9]	Deterrence theory		✓		✓		
D'Arcy and Herath [14]	Deterrence theory				✓		
Ali et al. [13]	Behavioral transformation (Insider behavior)		✓			✓	
Tsohou and Holtkamp [17]	Security compliance (Insider behavior)					✓	
Zandesh et al. [18]	Healthcare in the cloud			✓			
Hina and Dominic [15]	Higher education institutions		✓	✓			
Palanisamy et al. [16]	BYOD		✓				
This Study	Requirements, Policies and Impacting Factors	✓				✓	✓

Journal Pre-proof

While prior review works deliver valuable insights on focused topics in information security, theory applications, behavioral issues, context specific; there is a lack of review work that provides broader analysis of compliance requirements and their corresponding stakeholders and industries; policies and challenges they address; and impacting factors along with their scope of impact. Having such an investigation can bring an understanding of existing research focus, theories being used, evolving concepts and potential research directions. Accordingly, after analyzing the existing reviews shown in Table. 1, the study derives the three research questions (RQ1, RQ2, and RQ3), as mentioned in the introduction.

3. Methodology

We adapted the method of Kitchenham et al. [19] for conducting the systematic literature review. The method of Kitchenham et al. [19] uses evidence-based thinking for identifying and synthesizing the existing body of knowledge. It provides guidance that helps identifying, analyzing, and reporting relevant studies in an objective and replicable way. Our review protocol has been designed accordingly and is elaborated on in this section. Fig. 1. shows the steps followed to execute this study.

Firstly (Step 1), we set the objective of the review. Based on that, a set of keywords were used to formulate search queries (Step 2). The queries are then executed to retrieve only review articles (Step 3), which are relevant to the objectives of our study. It contributes to establishing a foundational background and link related findings, ensuring that the research questions to be developed have not been addressed in existing research. After analyzing the collected review articles (Step 4), we derived the research questions and improved keyword sets (Step 5). The results of these five steps were shown in Section 2 of this study.

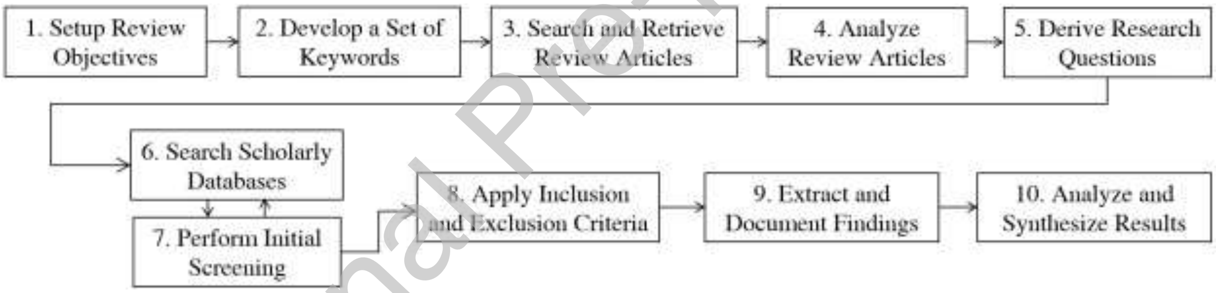

1. Setup Review Objectives
2. Develop a Set of Keywords
3. Search and Retrieve Review Articles
4. Analyze Review Articles
5. Derive Research Questions
6. Search Scholarly Databases
7. Perform Initial Screening
8. Apply Inclusion and Exclusion Criteria
9. Extract and Document Findings
10. Analyze and Synthesize Results

Fig. 1. Steps Followed to Conduct the Review

In the next step (Step 6 of Fig.1; Step 1 of Fig. 2), we execute the search query in scholarly databases to collect primary studies. The search terms used to retrieve the primary studies are: *("software compliance") OR ("compliance of software") OR (compliance AND "information systems") OR (compliance AND "distributed systems") OR (compliance AND "software systems") OR (compliance AND "service-oriented systems")*. These search terms cover various alternative names of a software besides having the asterisk symbol in (*compliance) and (system*) retrieves articles that discuss compliance as well as noncompliance, and likewise for systems. We believe that the above mentioned terms are sufficient enough for representing the topic. The search query is customized according to the syntax of the corresponding scholarly databases, in order to retrieve as many results as possible and eliminate chances of missing relevant articles. The table in Appendix A shows the scholarly databases and their correspondent queries executed. The selected databases are Google Scholar, Web of Science, ScienceDirect, Scopus, ACM Digital Library, and IEEE Xplore. A detailed explanation of this step is shown in Fig.2 (Steps 1 to 3) with the number of results retrieved. The reduction from 8,203 articles to 4,772 is due to considering the publication period (2011-2021), as specified in the inclusion criteria as well. For this, Zotero version 5 has been used as a referencing tool for managing, and organizing the references of the retrieved studies. This Step 6 goes in parallel with performing an initial screening of the results (Step 7 of Fig.1; Step 4 of Fig.2), in which titles and abstracts are checked with respect to their relevance to the review questions. The initial screening reduces the number of articles to 637. After removing duplicate articles, the total number of articles is reduced to 484 (Step 5 of Fig.2).

After finishing the initial screening, we applied a more rigid set of inclusion and exclusion criteria (Step 8), to further reduce the number of studies to a focused, highly relevant, and manageable amount of primary studies (Step 8 of Fig.1; Step 6 of Fig.2). The following inclusion and exclusion criteria have been used to achieve that all relevant software compliance studies are found:

- ***Inclusion criteria:***
    - Research articles published in international peer reviewed outlets. This is to ensure the scientific quality of primary studies.
    - Full research work is considered, such that the contribution is clearly tested and evaluated.
    - Published between 2011 to 2021. This publication period has been set to the last 10 years only, acknowledging the high dynamicity of software technologies. Considering the most recent studies is crucial to bring more focus on contemporary settings.
    - Relevant to the objective of the study. In other words, the study discusses at least one of the research questions in order to be eligible for selection.
    - Conference articles between 2011 and 2016 that have more than or equal to 30 citations in Google Scholar. We set this threshold for conference publications, in order to, on the one hand, reduce the number of retrieved studies within that period and, on the other hand, to pay attention to the most influential articles during that period. As described in Section 4.1 and the figure in Appendix E, this threshold of 30 citations is appropriate.
- ***Exclusion criteria:***
    - Studies in which "Software Compliance" has only marginal relevance, not a focal point of discussion. In other words, if the main objective of a primary study is not on compliance of E-type software, the study is excluded.
    - Non-English articles due to limitation of accessing and interpreting scholarly articles written in languages other than English.
    - Reports, book chapters (however, if the book chapters were conference contributions, they are included in the analysis), presentation materials, posters. We exclude these, because they usually tend to cover early results, to summarize research work, and some of them do not go through the scientific review process.
    - Conference articles between 2011 and 2016 that have a number of citations less than 30 in Google Scholar. Since articles published in that period are slightly older, we consider the number of citations as a metric that represents how influential an article is. This threshold of 30 citations is appropriate, as described in Section 4.1 and Appendix E.

The result of applying the inclusion and exclusion criteria are 77 research articles (primary studies). Following that, the data extraction is performed (Step 9 of Fig.1), in which Microsoft Excel has been used. Finally, for analysis (Step 10 of Fig.1); we used keyword co-occurrence, bubble plot mapping, content aggregation and vote counting technique, for which VosViewer and Microsoft Excel have been used. These steps provide a rigorous method for reproducing the literature review, while thoroughly laying the foundation for addressing the three RQs.

Journal Pre-proof

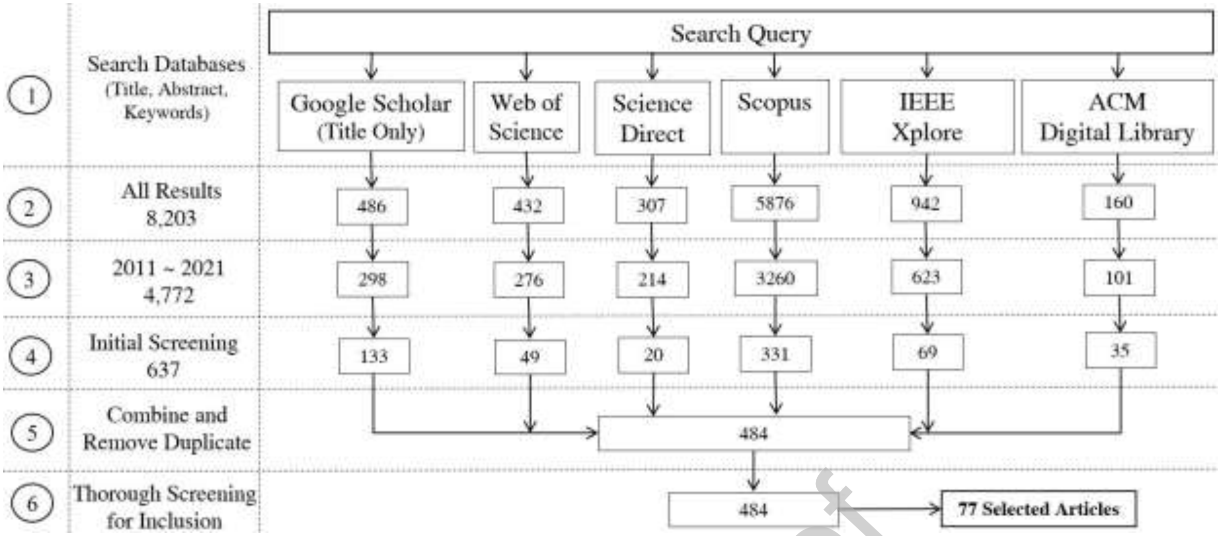


Fig. 2. Steps Executed for Reduction and Selection of Relevant Articles for the Review

4. Analysis of Results

4.1 Descriptive Analysis

We generated a keyword co-occurrence of the selected 77 articles using VOSViewer (version 1.6) to analyze top keywords and clusters discussed in the field. The threshold of keyword co-occurrence is set to a minimum number of occurrences at least twice. The co-occurrence refers to the words that are mentioned by more than one article's keyword list. In our selected articles, VOSViewer identified 42 keywords that appeared at least two times in the keyword list, forming 6 clusters (Fig. 3) generated based on the built-in clustering technique developed by Van Eck and Waltman [20]. The topics of each cluster is indicated in the legend of Fig.3.

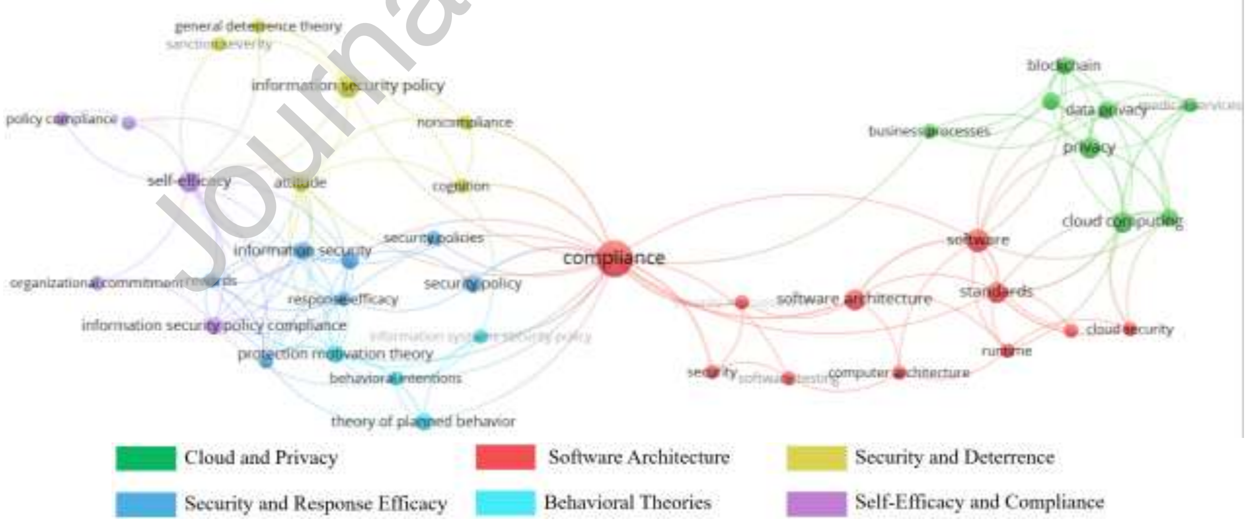


Fig. 3. VOSViewer Analysis of Keyword Co-occurrence

In addition to co-occurrence of keywords, the analysis also shows the total link strength of these keywords. The total link strength represents the number of articles in which two keywords occur together

Journal Pre-proof

[20]. The following are the top 10 co-occurred keywords and their total link strength shown in Fig. 4.: Compliance, Software, Information Security Policy, Self-Efficacy, Cloud Computing, Privacy, Standards, Software Architecture, Protection Motivation Theory, and Attitude. The high occurrence and strong linkage of these keywords indicates the importance of these topics in the context of software compliance.

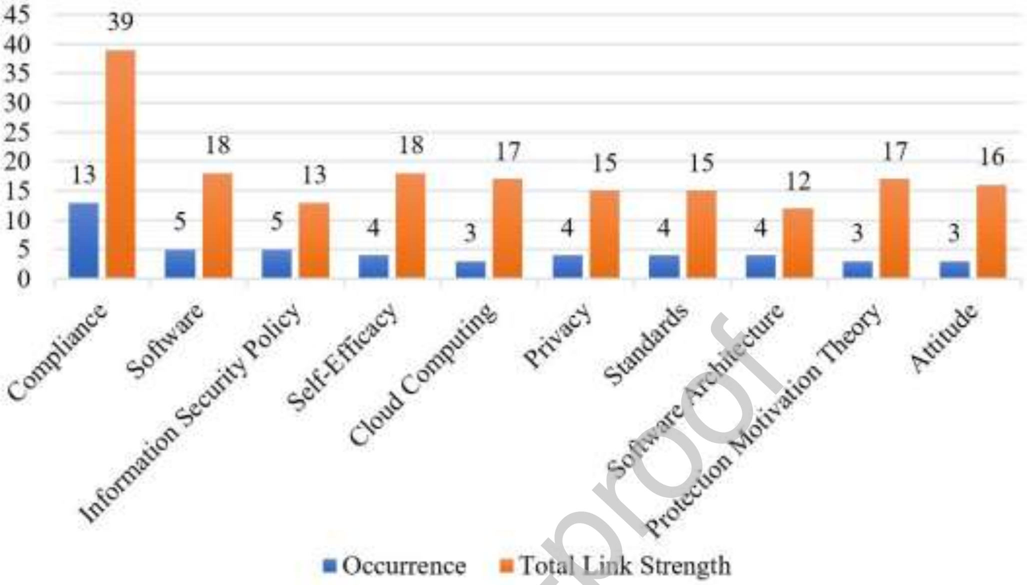


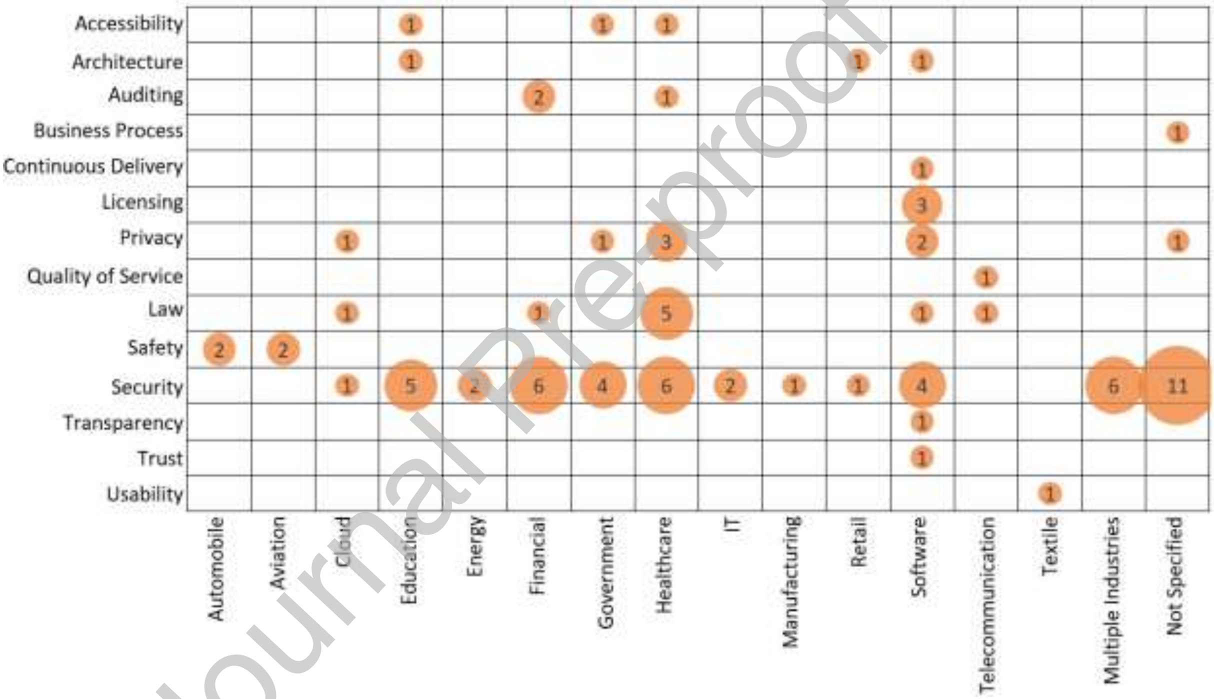
Fig. 4. Top 10 Co-occurred Keywords and their Total Link Strength

The table in Appendix B shows the publishers and the number of primary studies for the different publication types. Overall, there have been 60 journal articles, 14 conference papers, and 3 workshop papers. The distribution of articles based on the country of the study is shown in the figure in Appendix C. While 29 articles do not specify the countries in which the studies have been conducted, the remaining 38 articles state the countries of their studies. The colored legends in the map show the number of articles with regard to respective countries. For example, the dark blue legend represents countries with 8 publications, the United States is on the top of the list followed by China, Canada, and Malaysia. While most of the primary studies are conducted in a single context, several studies consider more than one. The studies, which are conducted in more than one context are: Guhr et al. [4], Castellanos-Ardila et al. [21], Máñez-Carvajal et al. [22], Diamantopoulou & Mouratidis [23], Granlund et al. [24], Karjalainen et al. [25]. The distribution of the number of articles according to their year of publication is depicted in the figure in Appendix D, demonstrating that the interest in the topic is still increasing during the past 5 years. The low number of publications for the year 2021 could be the result of delayed availability of publications. The figure in Appendix E shows that the threshold of 30 citations for conference publications for the years 2011 to 2016 is appropriate, as the linear regression (y = - 8.0766 x + 16334) on the years 2017 to 2021 results in an estimated number of citations of 51.6 for the year 2016. A value way higher than the threshold of 30 citations that has been applied to conference publications.

4.2. Compliance Requirements and their Respective Industries and User Contexts

With regard to research question RQ1 (What are the software compliance requirements with respect to different industries and user contexts?), our review analyzed these requirements at a categorical level using bubble plots to simplify the mapping of requirements and their corresponding industries and user contexts. The compliance requirements are derived based on the statements made in the primary studies with respect to their foci and the aspects of compliance that they intend to address. The analysis shows that the security requirement is the most discussed issue in many industries including healthcare [26]–[31], finance [32]–[37], education [35], [38]–[41], software [12], [42]–[44], government [34], [45], [46], energy [47], [48], IT [34], [35], manufacturing [34], retail [35], and cloud services [49].

The second most discussed topic are legal requirements in the field of healthcare [24], [50]–[53], software [54], finance [52] cloud [55] and telecommunications [56]. Privacy requirements are addressed in industries including healthcare [23], [57], [58], software [59], [60], government [23], and cloud services [57]. Licensing is highly connected to the software industry [61]–[63]; while auditing is discussed in financial [37], [64] and healthcare [27] sectors. Safety is discussed in the context of the aviation [21], [66] and automobile [67], [68] industry. Accessibility is discussed in government [69], healthcare [70] and education [22] sectors. Fig. 5 depicts the industries and their corresponding compliance requirements.



Journal Pre-proof

Fig. 5. Distribution of Selected Studies Based on Industry and Compliance Requirements

The analysis shows that different requirements could represent different levels of importance to the corresponding industry. Nevertheless, security is a critical requirement for most industries. Software compliance is less of an issue for business processes, continuous delivery, quality of service, trust and transparency. With regard to different industries, manufacturing, retail and textile are found to be the most indifferent to compliance.

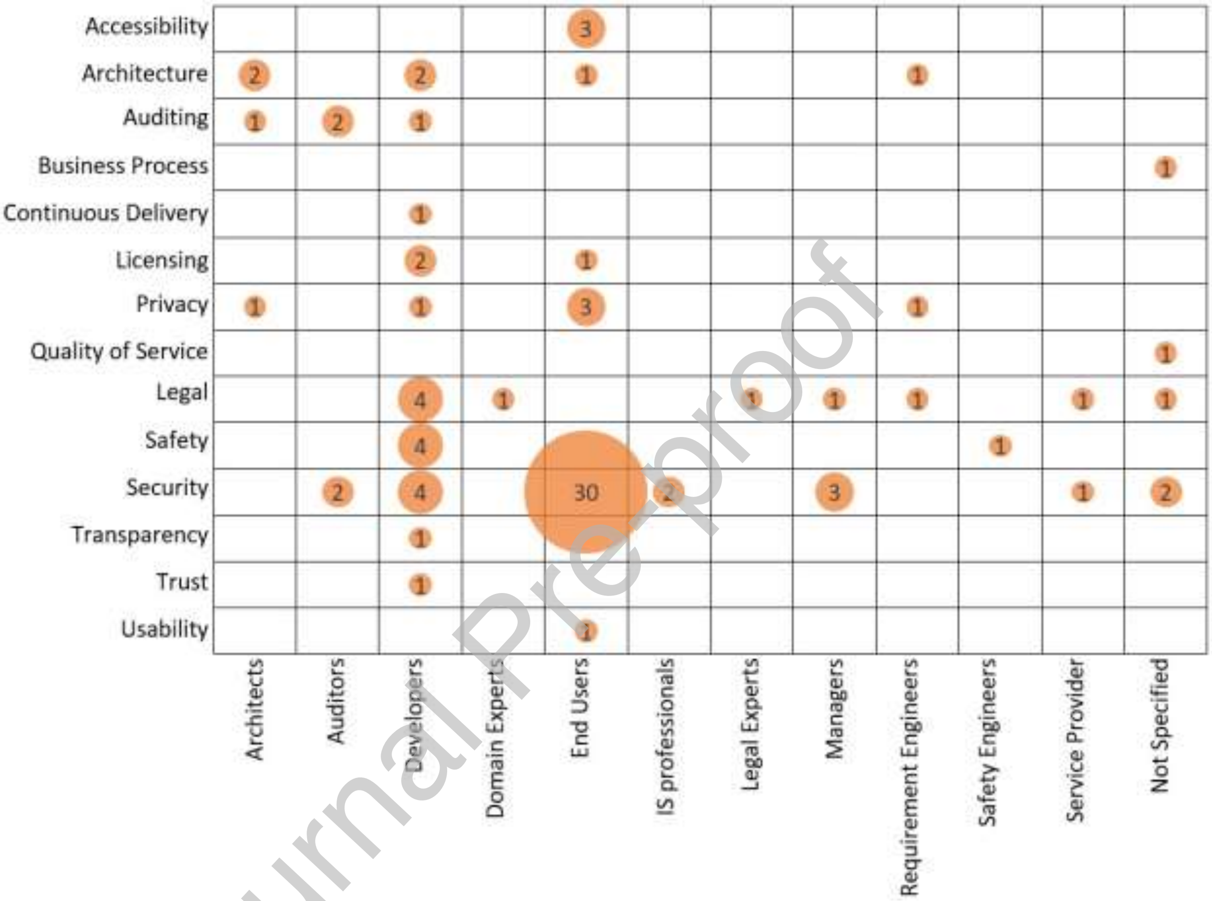
Regarding compliance requirements and their associated types of users, most studies deal with issues related to security compliance of end users [4], [25]–[35], [38]–[41], [45], [46], [46]–[49], [71]–[80]. End users are also associated with other requirements including privacy [23], [58], [81], accessibility [22], [69], [70], usability [82] and licensing [62].

Developers are the second highly discussed, and they are concerned more with security [12], [36], [43], [44], legal requirements [51], [52], [54], [56], safety requirements [21], [66]–[68], licensing [61],

Journal Pre-proof

[63], software architecture [83], [84], privacy [57], transparency and trust [85].

Managers, auditors and architects are discussed less compared to end users and developers. Managers are discussed in relation to security requirements [86]–[88] and legal requirements [56]. Auditors are also addressed in the context of security [37], [42] and auditing [37], [64]. Software architects are discussed in relation to architecture [83], [84], auditing [64] and privacy requirements [59]. The analysis also shows other stakeholders that are discussed however, to a very less extent, see Fig. 6.



Journal Pre-proof

Fig. 6. Distribution of Studies Based on Type of Users and Compliance Requirements

Based on the reviewed articles, the analysis reveals a high concern regarding end user security compared to other stakeholders. Most requirements were addressed to end users and developers who are in the forefront of developing or using a software system. The least paid attention stakeholders are the domain and legal experts, and safety engineers.

4.3. Factors Impacting Software Compliance

Before discussing the impacting factors, it is crucial to deliver an overview on the foundational theories and concepts used by the selected studies, as shown in Fig. 7. The theory of planned behavior is on top of the list followed by deterrence and protection motivation theories. Other concepts and theories, which are discussed at least twice include: requirement engineering [24], [50], [52], [54], [56], [65]–[67], [89], privacy-by-design [23], [59], [60], [81], rational choice theory [31], [32], [79], [88], social bond theory [26], [45], [47], [87], ontology [12], [55], [58], design principles [22], [70], neutralization theory [38],

[90], organizational climate theory [26], [88], theory of workarounds [82], [91], and compliance-by-design [21], [64]. The table in Appendix F lists the theories, the references to those theories, and the primary studies using them.

There are also other theories used by the primary studies. However, they seem applicable to a less extent as they have been used only once in the primary studies. The references for these theories are also listed in the table in Appendix F. The primary studies using them are: affective events [77], reasoned actions and cognitive evaluation [92], cognitive moral development [31], technostress, moral disengagement, and coping [73], discourse analysis [28], ethical decision making [38], ethical work climate and expected utility [63], expectancy [72], information system security [71], mangle of practices [80], reactance [78], regulatory compliance [69], self-determination [34], social exchange (guanxi) and technology threat avoidance [76], social learning [93], unified model of information security policy compliance [74], upper echelon [30], value neutrality [25], value-based compliance [29], and work system theory [82].

It is important to highlight the aforementioned theories and concepts used by the primary studies as they constitute a foundational understanding of the software compliance domain, based on the identified studies. In other words, theories and concepts provide a deeper explanation and interpretation of the factors being identified in our review which, in turn, allows for a better control of these factors when it comes to policy design.

Journal Pre-proof

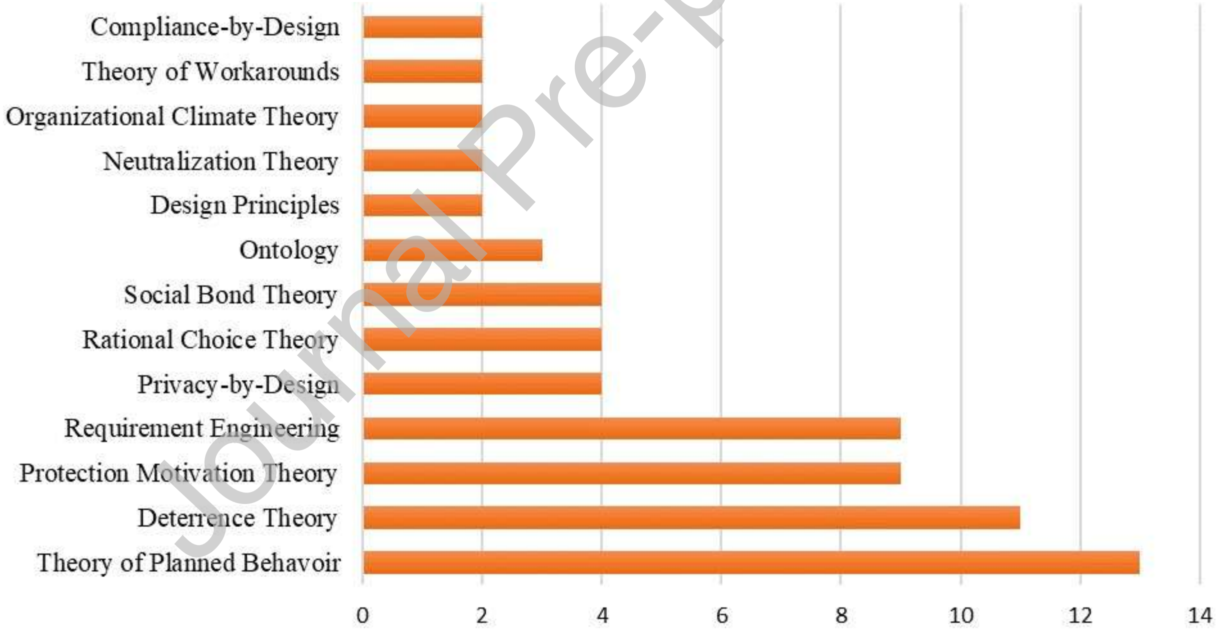


Fig. 7. Foundational Concepts and Theories Discussed Most by Selected Studies

To answer the research question RQ2 (What are the factors that impact software compliance, and which aspects of compliance are impacted?), our review, which is inspired by the theory of planned behavior [94], finds that the identified factors from the primary studies are mainly impacting three behavioral aspects: compliance attitude, compliance intention, and compliance behavior. Although the attitude and intention can be good predictors of the behavior, they may not necessarily result in the actual compliance behavior [95]. Based on that, these three aspects were used to group the number of research articles, which study the impact of a factor on these aspects. Additionally, we present the scope of impact (i.e., individual, organizational, or cultural) for each factor, to provide a further understanding of the context, in which those factors impact. In order to simplify the representation, our review uses a vote counting approach for synthesizing and presenting the results [19].

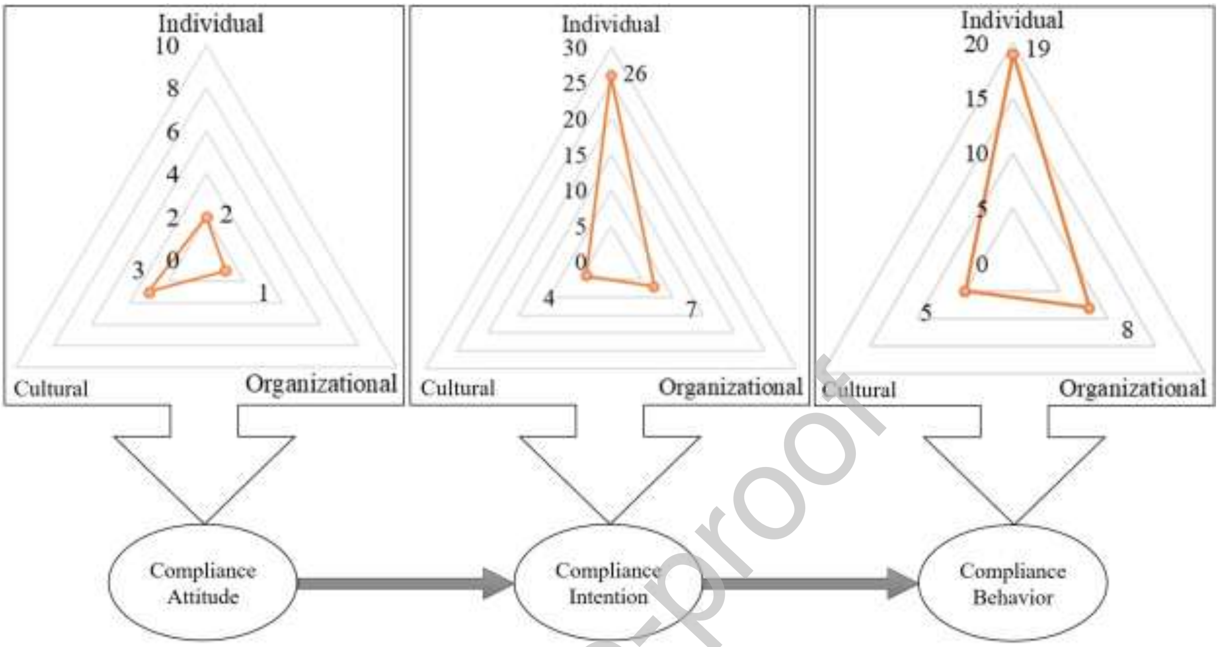


Fig. 8. Scopes and degree of impact of the identified factors

Journal Pre-proof

Fig. 8 presents a high-level overview of the scopes (i.e., individual, cultural and organizational) and degree of impact for all three aspects (i.e., compliance attitude, compliance intention, and compliance behavior). The figure shows that attitude towards compliance is impacted more by cultural factors, which indicates that attention should be paid to address cultural factors due to their contribution towards shaping the compliance attitude. Organizational factors seem to have a lesser impact on compliance attitudes compared to cultural ones. The compliance intention and the compliance behavior are impacted more by individual factors, while the organizational factors come second.

We identified 66 factors, which the primary studies empirically investigated. Among those, 11 factors (gender, fear, perceived behavioral control, social pressure, technical countermeasures, passive/avoidant leadership, transactional leadership, differential reinforcement, detection probability, information security policy, perceived effectiveness of measures) were reported to have insignificant impact on the compliance aspects and, therefore, were excluded in our analysis. The remaining 55 factors were reported in the primary studies to have a positive or a negative impact (Table.2). In the following subsections, we discuss these factors in detail.

Table 2. Factors impacting different aspects of compliance and their respective scope of impact
+ positive impact, - negative impact, Ø insignificant impact. The number of occurrences indicates the number of studies saying so.

#	Factors	Base Theory	Scope of Impact			Impacted Aspects		
			Individual	Cultural	Organizational	Compliance Attitude	Compliance Intention	Compliance Behavior
1	Abusive Supervision				✓		+	

2	Punishment	Deterrence			✓		+ + + +	+
3	Rewards	Compliance			✓		+ Ø Ø	
4	Certainty of Control	Deterrence			✓		+	
5	Security-Related Stress	Technostress	✓				-	
6	Moral Disengagement	Moral Disengagement	✓				-	
7	Top Management Support and Beliefs	Organizational Climate			✓			+
8	Cost-Benefit Analysis	Rational choice	✓					-
9	Sanctions	Deterrence			✓	+	Ø	+ +
10	Self-Efficacy	Protection Motivation	✓				+ + + + + + Ø	+ + +
11	Descriptive Norms	Social Norms		✓		+	+	+
12	Differential Association	Social Learning		✓				-
13	Imitation	Social Learning	✓					-
14	Moral Norms	Planned Behavior		✓				+
15	Security Valence	Expectancy	✓				+	
16	Security Instrumentality	Expectancy	✓				+	
17	Security Expectancy	Expectancy	✓				+	
18	Transformational Leadership	Full- range Leadership			✓		+	
19	Procedural Countermeasures	Intellectual capital cyber security			✓		+	
20	Socio-Cultural Environment	Information Systems Security		✓			+	
21	Neutralization	Neutralization	✓				- -	
22	Attitude Towards Compliance	Planned Behavior	✓				+ + + + + + + +	+ + +
23	Normative Beliefs	Planned Behavior		✓			+	+

Journal Pre-proof

24	Response Efficacy	Protection Motivation	✓				+ + + Ø Ø	+
25	Perception of Compliance Benefits	Rational Choice	✓				+	+
26	Perception of Compliance Cost	Rational Choice	✓				- - Ø	- - Ø
27	Perception of Noncompliance Costs	Rational Choice	✓				+	+
28	Attachment	Social Bond	✓				+	
29	Commitment	Social Bond	✓				+	+
30	Involvement	Social Bond	✓				+	
31	Personal Norms	Planned Behavior	✓			+	+	
32	Perceived Trust		✓					+
33	Compliance Behavioral Beliefs	Planned Behavior	✓				+ +	
34	Compliance Knowledge	Social cognitive	✓				+	
35	Subjective Norms	Planned Behavior		✓		+	+ + + Ø	+
36	Religion	Cognitive moral development	✓					+
37	Personality Traits	Protection Motivation	✓					+
38	General Information Security		✓					+
39	Technology Awareness				✓			+ Ø
40	Negative Affective Flow	Affective flow	✓					- Ø
41	Perceived Severity of Threat	Protection Motivation	✓				+ + Ø	+
42	Perceived Vulnerability	Protection Motivation	✓				+ + +	+
43	Personal Capabilities	Planned Behavior	✓					+
44	Locus of Control	Social Cognitive	✓				+	
45	Social Norms	Social Norms		✓		+		+

Journal Pre-proof

46	Information Security Climate	Organizational Climate			✓			+
47	Information Security Training				✓			+
48	Compliance Intention	Planned Behavior	✓					+
49	Perceived Digital Mutualism Justice	Organizational Justice	✓				+	
50	Perceived Freedom Threat	Reactance	✓				-	
51	Perceived Responsibility		✓				+	
52	Work Impediment		✓				-	
53	Supervisor-Subordinate Guanxi	Social exchange			✓			+
54	Perceived Threat	Protection Motivation	✓				+	Ø
55	Ethics		✓			+		

4.3.1. Factors Influencing Compliance Attitude

Based on the 77 reviewed papers, the attitude towards compliance is influenced by several factors: personal norms; ethics; descriptive, social, and subjective norms; and sanctions. We discuss these in detail based on their scope of impact: individual, cultural and organizational. The low number of articles and factors that impact the attitude towards compliance indicate that further research can look into other aspects and factors that shape and influence compliance attitude.

4.3.1.1. Individual

Personal norms and ethics are critical to shaping the compliance attitude. *Personal Norms*, which refer to values an individual has, can provide a moral obligation of oneself towards compliance [41]. *Ethics* also act as a guidance and moral principles and therefore influences to a great extent the attitude towards compliance [62].

4.3.1.2. Cultural

Descriptive, social and subjective norms contribute to the attitude towards compliance. *Descriptive Norms* motivate the compliance attitude based on one’s perception that other people are complying [41]. The same goes for *Social Norms*, which are informal rules guiding a certain behavior and influences the attitude. *Subjective Norms*, which represent the likelihood that significant others (i.e., friends, colleagues, surrounding people) approve a certain behavior, can play a critical role in the development of compliance attitude [41].

4.3.1.3. Organizational

Sanctions, whether organizational or legal, can help direct the attitude towards compliance in a positive

Journal Pre-proof

way. They refer to the consequences that employees believe to result when failing to comply with policies[62].

4.3.2. Factors Influencing Compliance Intention:

Based on the reviewed papers, there is more attention paid to compliance intention than other aspects of compliance. The factors impacting the intention are: security-related stress, moral disengagement, self-efficacy, security valence, security instrumentality, security expectancy, neutralization, attitude towards compliance, response efficacy, perception of compliance benefits, perception of compliance cost, perception of noncompliance costs, attachment, commitment, involvement, personal norms, compliance behavioral beliefs, compliance knowledge, perceived severity of thread, and perceived vulnerability, locus of control, perceived digital mutualism justice, perceived responsibility, perceived threat, descriptive norms, socio-cultural environment, normative beliefs, and subjective norms, abusive supervision, punishment, rewards, certainty of control, transformational leadership, and procedural countermeasures. The behavioral intention of compliance is well explored in the literature from an individual perspective. However, from a cultural and organizational perspective, further confirmation of some factors is needed to strengthen the findings and enhance the likelihood of generalization.

4.3.2.1. Individual

Self-Efficacy, which is the confidence in one's capacity to control, has a positive and significant impact on compliance intention [34], [39], [40], [86], [87], [92]. Similarly, *Response Efficacy,* which refers to the perceived effectiveness of responses to incidents, is reported by three studies to have a positive impact [78], [86], [90]. However, Siponen et al. [92] and Hina et al. [40] reported an insignificant impact of response efficacy on compliance intention, justifying that by the lack of users' involvement in formulating security policies.

Security Valence and *Security Instrumentality* positively influence compliance intention [72]. While security valence reflects an insider's preference [96] and perception of how attractive policies are, security instrumentality is the perception of how securing user's information can protect an organization from potential threats [72]. The same study by Burns et al. [72] reported that *Security Expectancy*, that is the perception of one's effort to carry out protective behaviors, positively impacts compliance intention.

Attachment to organizational peers, *Commitment* to its goals, and *Involvement* in organizational activities can enhance the social bond of an individual and positively impact the intention to comply [47].

Availability of *Compliance Knowledge* is crucial to users' perception of compliance related issues [48], since it contributes to enhancing their intention to comply. These include: *Perception of Compliance Benefits* and *Noncompliance Costs* [90], *Perceived Threat* [78], *Perceived Severity of Thread* [40], [92], *Perceived Vulnerability* [40], [86], [92], *Perceived Responsibility* [34], and *Perceived Digital Mutualism Justice* [78]. Developing such a perception requires organizations to invest in training and awareness programs [48].

Locus of Control, which represents users' ability to control the events that affect them, empowers individuals to take responsibility for their actions and, therefore, enhances their intention to comply [87].

Personal Norms can provide guidance of one's beliefs and intentions towards organizational policy compliance. They constitute an individual's values and views; thus, they significantly contribute to one's intention to comply [47].

Attitude Towards Compliance is strongly confirmed by several studies to positively impact intention to comply [26], [40], [41], [63], [86], [87], [90], [92]. This indicates that addressing various aspects that shape compliance attitudes improves the overall compliance. Although behavioral beliefs in the theory of planned behavior impacts the attitude [94], *Compliance Behavioral Beliefs* were reported to positively impact the intention to comply [48], [92].

Security-Related Stress refers to the stress caused by demand imposed by security requirements [73]. The concept is mainly derived from Ragu-Nathan et al. [97] technostress. The security-related stress can lead to *Moral Disengagement* from appropriate behavior to cope with such stress. As a result both contribute to negatively impact the intention to comply [73].

Neutralization refers to the justification of deviant behavior to substitute the feeling of guilt associated with that behavior using neutralization strategies. These include denial of injury, loyalty, condemnation of condemners, metaphor of the ledger, necessity, and defense of ubiquity [98]. Rationalization of noncompliant behavior can encourage more violation of policies and thus negatively impact the compliance intention [38].

Perception of Compliance Costs, which is the time and efforts needed for compliance, can be seen as a burden to productivity and, therefore, negatively influences compliance intention [39], [90]. However, Ifinedo [86] reported an insignificant impact with a justification that it all depends on one's cost-benefit perception of compliance rather than on compliance cost alone.

Perceived Freedom Threat, which concerns limiting a user's freedom to choose actions related to their own device. This can have negative consequences on their intention to comply since they expect no restriction or control on their own devices [78].

Work Impediment refers to constraints or interferences in the way towards task completion. Examples are redundant workflows or excessive security procedures. This can be cumbersome and consumes time, which in turn motivates bypassing policies and working around prescribed workflows; thus, it negatively impacts one's intention to comply [34].

4.3.2.2. Cultural

Descriptive Norms represent how people typically act or think towards a certain behavior [99]. In a relatively similar concept, *Normative Beliefs* indicate the extent at which important surrounding members think of what should or should not be done towards a certain behavior [100]. Both descriptive norms and normative beliefs positively contribute to impacting intention to comply [39], [90].

Subjective Norms, which indicate the extent to which the majority of members approve a certain behavior, have a strong positive impact on compliance intention [63], [86], [87]. However, Hina et al. [40] found an insignificant impact of subjective norms on the intention to comply. Their study justifies such a finding with the possibility that a certain behavior might not be influenced by peers if the culture of that behavior is not well established.

Establishment of a *Socio-Cultural Environment* can help in developing a culture of compliance through influencing habits and organizational citizenship in the long run and, in turn, positively impact compliance intention [71].

4.3.2.3. Organizational

Abusive Supervision can create a negative attitude and resistance to compliance [75]. However, it was reported to be effective for building a commitment towards organizational policies, and as a result mitigate intention to violate [75]. Generally, leadership plays an important role in incentivizing compliance. A particular type is *Transformational Leadership* which stimulates employees to put their organizational interests ahead of their own interest. It goes beyond achieving performance to optimize the

Journal Pre-proof

overall development and innovation of an individual, group and organization. This can have a strong and a positive impact on employees' intention to comply [4].

Procedural Countermeasures including development of policies and awareness programs can play an extrinsic role in guiding the intention towards compliance. Technical countermeasures themselves are not sufficient, since human behavior is unpredictable [71].

Punishment and *Rewards* have an interplay effect on their impact towards compliance intention, and both were reported by primary studies to have a positive impact [30], [33], [45]. However, Siponen et al. [92] reported an insignificant impact of rewards on the intention to comply. The study justifies that some organizations do not give rewards for complying with policies, because employees are required to comply [92]. Additionally, based on a study in an education institution by Bansal et al. [38], gender can play a role in intention to noncompliance. However, the significance of that role depends on neutralization techniques used to justify the noncompliance in a specific context.

Certainty of Control refers to the likelihood of enforcement strategy of policies. This can trigger a signal to employees that their activities are being monitored, evaluated, and punished for noncompliance to policies. Accordingly, their intention to comply increases [33].

Journal Pre-proof

4.3.3. Factors Influencing Compliance Behavior

Compliance behavior is well investigated among the selected studies, identifying many factors at different scopes, these are: cost-benefit analysis, self-efficacy, imitations, attitude towards compliance, response efficacy, perception of compliance benefits and costs, perception of noncompliance costs, perceived trust, religion/morality, personality traits, general information security, negative affective flow, perceived severity of threat, perceived vulnerability, personal capabilities, compliance intention, descriptive norms, differential association, moral norms, normative beliefs, subjective norms, social norms, punishment, top management support and beliefs, sanctions, technology awareness, information security climate, information security training, supervisor-subordinate guanxi, organizational commitment. While well investigated, further confirmation of some factors is needed to strengthen the findings and enhance the likelihood of validity and generalization.

4.3.3.1. Individual

Self-Efficacy strongly and positively motivates compliance behavior of an individual [27], [31], [46]. Similarly, *Personal Capabilities*, which refer to one's knowledge and competence, encourages compliance behavior [32].

Personality Traits such as openness, agreeableness and extraversion can spillover certain values and give a strong impact on compliance behavior according to a limited sample of healthcare employees in a single hospital by T. Alanazi et al. [31].

Response Efficacy is an effective strategy that encourages employees to engage in compliant and responsible behaviors based on a study by Liu et al. [46] on public sector employees in China.

Perception of Compliance Benefits and *Perception of Noncompliance Costs* contribute to understanding the value gained by adherence and consequences resulting from noncompliance, and therefore, incentivize the compliance behavior [32]. On the other hand, *Perception of Compliance Costs* were reported to have a negative impact on the compliance behavior [32], [46].

Perceived Trust and confidence in implementing and enforcing software related policies positively impact compliance behavior according to a study on Malaysian healthcare employees by

Journal Pre-proof

Humaidi and Balakrishnan [27]. Similarly, *Commitment* of employees to organizational goals is crucial, and it influences compliance behavior [46].

Religion is reported to contribute to the moral development of an individual and enhance his/her compliance behavior based on a limited sample of healthcare workers at a single hospital in Saudi Arabia [31].

General Information Security represents the understanding of information security policies and their related issues and consequences. A good understanding of general information security positively influences one’s compliance behavior according to the study of T. Alanazi et al. [31], which is based on a limited sample of healthcare workers at a single hospital in Saudi Arabia.

Perceived Severity of Threat and *Perceived Vulnerability,* which are two main constructs of the protection motivation theory [101], were reported by Liu et al. [46], to enhance compliance behavior.

Attitude Towards Compliance is confirmed to have a strong and a positive impact on compliance behavior [32], [62], [77]. Although the attitude typically leads to an intention in order to predict the compliance behavior according to the theory of planned behavior [95], it is worth reflecting and testing the relationship from attitude to behavior in the recent update of the theory with a consideration of active procurement and approval goals in place. *Compliance Intention* is also reported by one study to have a positive impact on compliance behavior [92] as it is also confirmed by the planned behavior.

Cost-Benefit Analysis indicates an individual evaluation of costs and benefits gained or resulted from compliance. Such evaluation of costs and benefits have a negative impact on the compliance behavior according to a study by Ifinedo [88] in Canada.

Imitation and observation of a similar behavior is found to negatively influence the compliance behavior as per a study conducted in Germany by Lembcke et al. [93].

Negative Affective Flow, which indicates an individual's immersion on negative emotions, has a negative impact on compliance behavior [77]. The study of Ormond et al. [77] also concluded a significant impact in the context of users who experience high frustration, and insignificant impact in the context of those who experience less frustration.

4.3.3.2. Cultural

Our analysis reports that various types of norms including: descriptive, moral, and social norms contribute to shaping the compliance behavior. *Descriptive Norms* and *Moral Norms* were confirmed to positively impact compliance behavior [35]. Descriptive norms are the perception of whether other people perform a certain behavior [102], while moral norms are an individual's sense of moral responsibility or obligation to do or obstruct from a certain behavior [94]. Similarly, *Social Norms*, which represent acceptable behavior by a group of people, can have a direct impact on compliance behavior [62].

Furthermore, *Subjective Norms* [31] and *Normative Beliefs* [32], which represent how other people who are important evaluate a certain behavior, were reported to positively influence the compliance behavior. Studies evaluate the impact of these two factors in contexts of healthcare and financial industries consecutively.

Differential Association, on the other hand, has a negative impact on compliance behavior. It refers to the extent at which interacting with peers makes an individual learn certain values and attitudes which in turn impact his/her behavior [93].

4.3.3.3. Organizational

Punishment [31] and *Sanctions* [88], [93] can be very powerful deterrence mechanisms that positively

Journal Pre-proof

contribute to enhancing compliance behavior.

Top Management Support and Beliefs influence the compliance positively according to a study in Canadian context by Ifinedo [88]. Similarly, *Supervisor-Subordinate Guanxi*, which refers to creating personal ties and exchange of favors between supervisor and subordinates, in that a strong supervisor-subordinate can incentivize organizational commitment and enhance behavioral compliance according to a study by Liu et al. [76], which has been conducted on government employees in China.

Establishment of *General Information Security* guidelines and *Technology Awareness* programs can enhance to a great extent the compliance behavior [31], [32], [46]. In addition to that, the existence of *Information Security Climate* can enhance employees' compliance behavior, since it represents a collection of shared values, beliefs, and assumptions on information security among the organizational members. Moreover, according to Liu et al. [46], the information security climate is powerful and has a stronger effect on compliance than information security training.

The recent updates on the theory of planned behavior are brought in the name of *Reasoned Goal Pursuit*. Ajzen and Kruglanski [95] argue that the attitude can trigger the intention and is mediated by the motivation; the strength of that impact depends on how strong active procurement and approval goals are. None of the investigated studies has taken active procurement goals into account. Further studies should consider evaluating the compliance intention and behavior with respect to active procurement goals which represent the ultimate goal of performing such a behavior.

4.4. Policies and Addressed Compliance Challenges

To address research question RQ3 (What are the existing software compliance related policies and which compliance challenges do they tend to address?), this study aggregates the policies that are prescribed by the primary studies and compliance challenges they address. 19 policies were identified and are listed in Table 3. Most of these policies deal with end users and behavioral aspects of humans, while less policies focus on technology related challenges. Security education, training, and awareness (SETA) is at the top of the policies that many studies confirmed to be useful to promote compliance. Automation of compliance management for tackling challenges related to technology is the second to the top of the recommended policy.

Table 3. Policy Prescriptions and Addressed Compliance Challenges

Policy Prescription	Category	Addressed Compliance Challenges	References
Security education, training and awareness (SETA)	Human	Compliance and noncompliance intention, compliance and noncompliance behavior, organizational injustice, affective flow, engineers' sense of responsibility, non-malicious insiders, interpreting compliance requirements, functional safety, technostress	[27], [30]–[32], [39], [40], [47], [56], [60], [62], [67], [71]–[73], [75], [77]–[79], [86]–[88], [90], [92], [93]
Automation of compliance management	Technology / Human	Misconfiguration of infrastructure, efforts needed, accessibility checking, license compliance, potential security attacks, modeling regulations and standards into machine readable, misinterpretation of requirements by stakeholders, evolution of standards and regulations, neglection of best practices	[21], [22], [36], [44], [55], [56], [61], [83], [89]
Promoting organizational climate and social bonds	Human	Negligence, compliance intention, noncompliance behavior, compliance behavior	[25], [26], [39], [40], [47], [76], [87], [88]
Reward and punishment	Human	Negligence, insider breach, neutralization, noncompliance intention and behavior, resistance towards information security policy, divergence of preferences	[33], [35], [38], [41], [47], [87]
Internal control and auditing	Human	Adherence to security policy, information accountability, non-malicious insiders, security breaches, lack of transparency of	[30], [37], [58], [79], [85]

Journal Pre-proof

		distributed teams	
Deterring instruments	Human	Compliance intention, noncompliance behavior, compliance behavior	[39], [62], [88], [93]
Software certification	Technology	Interpretation of regulatory documents, enforcement of specific SDLC in MDD, requirement mismatches between physical devices and standalone device software, compliance with standards	[12], [24], [66], [67]
Regulation-oriented architecture	Technology	Data interoperability, regulatory compliance, gap between legal and technical experts, purpose limitation, accountability of the data controller, user right to erasure, and time-limited retention, gap between designers and auditors	[51], [53], [59], [64]
Model-driven development	Technology	Enforcing specific SDLC, diverse compliance sources, familiarity of business and compliance experts software engineering practices.	[66], [103]
Standardizing user accessibility	Technology	Usability, lack of accessibility	[22], [69], [70]
Investigating workarounds	Human	Insiders' behavior, inadequate information systems, shadow IT	[80], [82]
Analyzing rationalities behind noncompliance	Human	Noncompliance motivation, different rationalities, organizational injustice, affective flow	[29], [77]
Incorporating appropriate responses	Human	Detrimental compliance, compliance intention	[78], [91]
Establish codes of ethics	Human	Engineers' sense of responsibility	[60]
Evaluate security related stress	Human	Compliance intention, technostress	[73]
Practice-based discourse analysis	Human	Insiders' threat, workarounds, ambiguity of policies, employee prioritization	[28]
Applying most restrictive laws	Technology	Conflicting requirements, ambiguities, exceptions, contradictions	[52]
Outsourcing	Technology	Poor practices of in-house development	[42]
Runtime security auditing	Technology	Transparency, accountability, trust, and auditing of cloud infrastructures	[49]

We classify these policies into technology-related and human-related ones based on the nature of compliance challenges these policies tend to address (Fig. 9). The following subsections elaborate on these policies based on the proposed classification.

Journal Pre-proof

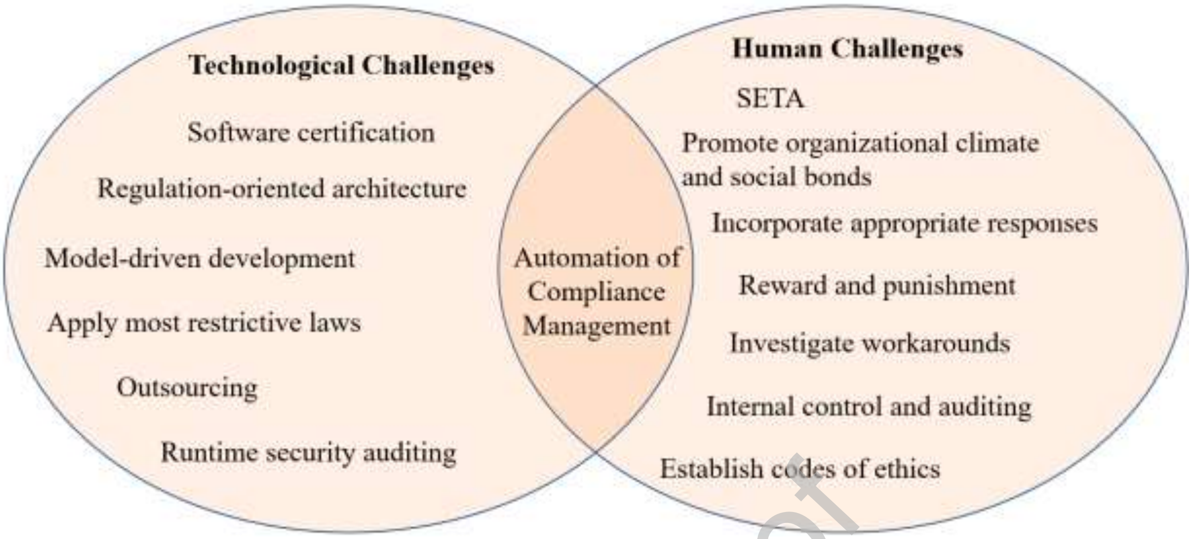

Technological Challenges
Software certification
Regulation-oriented architecture
Model-driven development
Apply most restrictive laws
Outsourcing
Runtime security auditing
Automation of Compliance Management
Human Challenges
SETA
Promote organizational climate and social bonds
Incorporate appropriate responses
Reward and punishment
Investigate workarounds
Internal control and auditing
Establish codes of ethics

Fig. 9. Classification of Policies based type of Compliance challenges they Address

Journal Pre-proof

4.4.1. Policies Addressing Human-Related Compliance Challenges

Various studies confirm that humans are the weakest point in software compliance, since their behavior and interactions with information security mechanisms is dynamic and unpredictable [80]. Therefore, many policies proposed to tackle user-related compliance challenges (Table 3), including automate compliance management, SETA, reward and punishment, internal control and auditing, investigating workarounds, promoting organizational climate and social bonds, development of deterrence instruments, evaluation of security related stress, establishing codes of ethics, analyzing rationalities behind compliance, and incorporating appropriate responses.

4.4.1.1. *Automation of Compliance Management* helps to a great extent to mitigate some of the manual compliance checking issues. Implementing such a policy makes the process of compliance management less error-prone and reduces the complexities associated with analyzing different sources of compliance requirements [83]. Besides that, the compliance management system can be used as a reference and guidance for compliance knowledge [48].

4.4.1.2. *Security Education, Training and Awareness (SETA)* is a powerful policy that an organization needs to pursue on a regular basis. Noncompliant behavior happens due to users' lack of knowledge [48], technostress [73], organizational injustice [77], [92], misinterpretation of requirements [56], users' negative emotions [77], or non-malicious insiders, who carry out noncompliance behavior unintentionally [79]. Several studies conclude that SETA helps mitigate noncompliance intention [73], [75] and noncompliance behavior [40], [88]. Through SETA, organizations can enhance compliance intention [30], [39], [71], [72], [78], [86], [87], [90], [92], and behavior [27], [31], [32], [47], [62], [86], [87], [93], [93].

4.4.1.3. *Promoting Organizational Climate and Social Bonds* through socialization and meetings leads to building a compliance culture in an organization and developing social norms [39], [87]. While the development of social norms and values in an organization needs investment in meetings and socialization [87]; the overall impact is mitigating noncompliance intentions and behaviors [40], [47], [88]. It helps to a great extent promote compliance behavior [25], [46], [87]; and reduce negligence and insider breach [26].

4.4.1.4. *Reward and Punishment* can be an effective tool to mitigate the impact of users' negligence [47], insider breach [33], and users' excuses for violation through neutralization strategies [33], [38]. Users by default are not motivated to follow certain procedures and policies [33]. Setting up a reward and punishment policy can minimize noncompliance intention [41] and behavior [47], [87]. Moreover, punishment indirectly reduces resistance towards information security policy [35]. While punishment on its own may not be enough to motivate compliance behavior, there found to be an interplay between punishment and reward [33].

4.4.1.5. *Internal Control and Auditing* is an effective policy that helps monitor users in terms of security practices and improve the overall adherence to information security policy [30] and information accountability [58]. This policy assists in identifying unsafe computer practices, non-malicious insiders [79], and security breaches [37]. It also addresses the issues of transparency in the activities of distributed teams [85].

4.4.1.6. *Deterring Instruments* play a nontrivial role in preventing security issues and enhancing compliance intention [39] and behavior [62], [93]. They can also help to a great extent mitigating non-deviant behaviors to policies [88].

4.4.1.7. *Investigating Workarounds* performed by insiders helps identify possible vulnerabilities and threats [80]. Workarounds are mostly triggered by inadequate information systems or complex security measures [82], that impact users' productivity especially when they are under pressure of meeting deadlines. As a result, this drives them to go around for an easier way to do their work while compromising policy measures. Investigating workarounds can reveal many compliance violations and acts which do not follow prescribed procedures.

4.4.1.8. *Analyzing Rationalities Behind Noncompliance* help understand the motivation of a certain behavior [29] and to develop effective policies. This policy can assist in revealing compliance issues that result from organizational injustice and users' negative emotions [77].

4.4.1.9. *Incorporating Appropriate Responses* to certain events needs to be considered since compliance, in some cases, can be detrimental and noncompliance, in other cases, can be beneficial depending on the context [91]. Therefore, it is crucial that organizations anticipate users' workarounds and incorporate appropriate responses [78], [91].

4.4.1.10. *Establishing a Code of Ethics* provides developers and engineers with guidelines and a valuable reference that help them meet industry standards and best practices. Such a policy can empower engineers and to enhance their sense of responsibility and accountability to deliver beyond just functionality [60].

4.4.1.11. *Evaluating Security-Related Stress*, which are caused by complexity and ambiguity of information security requirements, is crucial to reducing susceptibility to policy violation and threat [73]. While the concept of security-related stress is mainly inspired by technostress, we believe that evaluating the overall impact of technostress is of highly importance since it affects insiders' intention to comply.

4.4.1.12. *Practice-Based Discourse Analysis* helps address ambiguity of policies, employee prioritization and workarounds. In other words, if policies are developed in line with employees' work practices, there will be less room for workarounds and as a result less threat of insiders [28]. Such a policy is useful when policies are ambiguous or not compatible with employees' work practices. This ambiguity or incompatibility leads them to prioritize between such policies and their work practices; and in turn impacts their motivation towards compliance and encourages workarounds.

4.4.2. Policies Addressing Technology-Related Compliance Challenges

Our review also identified eight policies that are related to addressing technological compliance challenges. These are: automation of compliance checking, software certification, regulation-driven architecture, standardization of user accessibility, model-driven development, application of most

Journal Pre-proof

restrictive laws, runtime security auditing, and outsourcing (Table 3).

4.4.2.1. *Automating Compliance Management* addresses both human and technology related compliance challenges. From the technology side, it helps avoid errors and reduces time and efforts needed for checking compliance. Manual misconfiguration of complex software may result in security vulnerabilities [44]. Besides, the efforts needed to model compliance are significant, especially with a continuous evolution of standards and regulations [21]. Moreover, checking compliance with certain accessibility standards [22] or conducting a periodic assessment of risks [36] can be error-prone if done manually. In addition to that, there are duplicate efforts needed to manage diverse sources of compliance requirements [55]. This is likely to result in misinterpretation of compliance requirements by different stakeholders, therefore, automation of compliance checking is crucial to address such issues [83]. This is also obvious in the context that developers are less aware of compliance requirements [56]. Having a policy-as-code in place helps mitigate misinterpretation of requirements adding more efficiency and effectiveness to compliance management [89].

4.4.2.2. *Software Certification* with industry standards and best practices strongly minimizes risks and vulnerabilities, and simplifies managing compliance over the software life cycle. This ensures a proper implementation of security measures and conformance of integrated third-party components to security certification [12]. Certification also helps define compliance requirements for physical and virtual appliances [24], [67].

4.4.2.3. *Regulation-Driven Architecture* helps bridging the gap between legal and technical experts [53], since they tend to use different vocabularies and assumptions for analyzing information systems [64]. This approach allows privacy related settings to be embedded during the design [59]; and addresses interoperability issues of heterogeneous components [51].

4.4.2.4. *Model-Driven Development* simplifies dealing with and reflection of multiple sources of compliance requirements [103]. Continuous delivery of features becomes the norm in software development, the use of model-driven development paradigm helps bridge the gap between engineers and business and compliance specialists. Such a policy helps validate and enforce policies regardless of the software development life cycle approach followed [66]. This enhances efficiency in the long run and makes further development less sensitive to business and technology changes. Recent variations of this approach also include test-driven development and behavior-driven development.

4.4.2.5. *Standardizing User Accessibility* of a software maximizes users' usability and benefits, and in turn, impacting their performance and productivity [70]. On the other hand, poor design and lack of accessibility makes it hard for users to accept the system, prevents users from benefiting from the service, or at least impedes their productivity. For instance, following the web content accessibility guidelines (WCAG 2.0) can be established as a good reference for defining and checking usability and accessibility measures [22], [69].

4.4.2.6. *Applying Most Restrictive Laws* should be considered especially when there are conflicts, ambiguities, exceptions, or contradictions in requirements. Multiple regulations often include compliance requirements which govern the same or overlapping types of software systems. There is a possibility that a certain compliance requirement found in one legal text is more restrictive than the one found in another legal text [52]. Therefore, it is crucial that requirements engineers follow the more restrictive one to ensure that the system complies with both.

4.4.2.7. *Outsourcing* of software solutions can be a good option for the majority of organizations, since the complexity of software systems continues to increase [104], and the tendency of "assemble more, and code less" is becoming the norm. Thalmann et al. [42] discusses that in-house development can fail to

Journal Pre-proof

Journal Pre-proof

fulfill compliance compared to outsourced ones, following the line of argument that organizations outsourcing their IT need to enhance their service compliance, resulting in improved compliance. However, the more complex outsourcing is, the more difficult compliance management becomes for an organization [42].

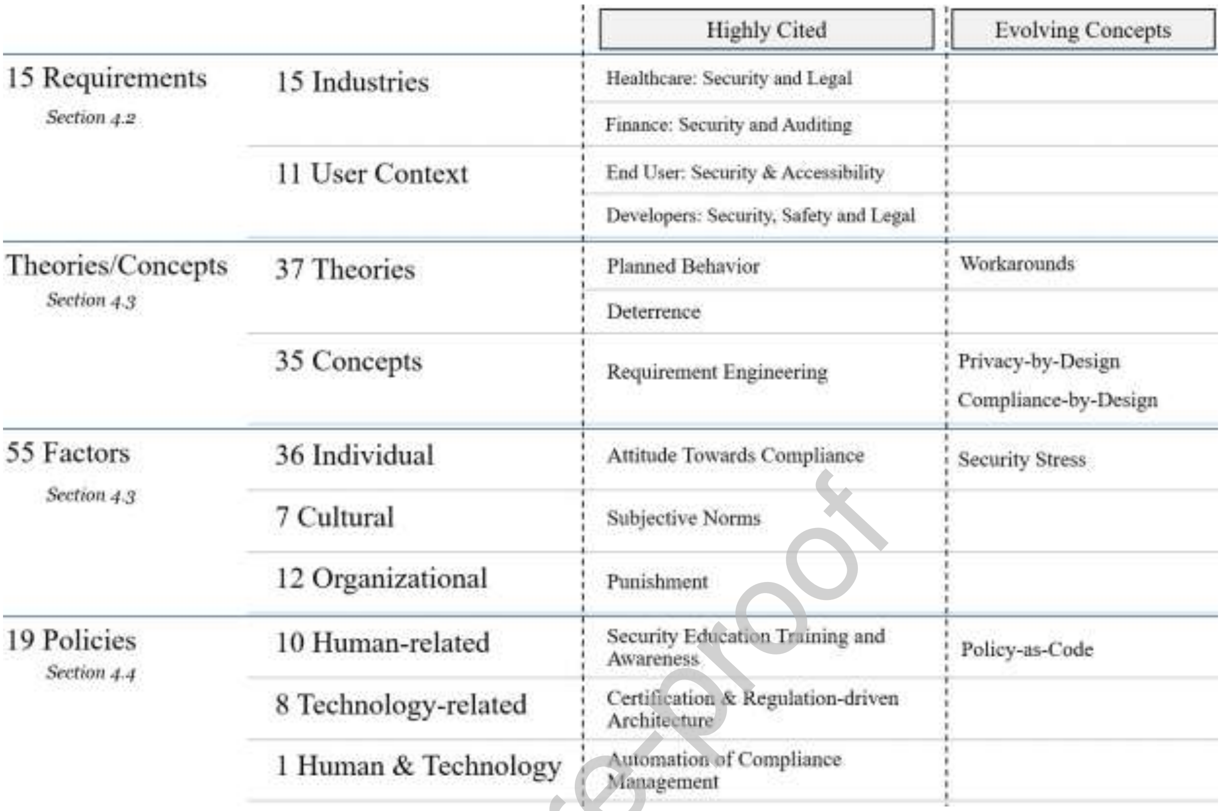
4.4.2.8. *Runtime Security Auditing* of a multi-tenant cloud environment is of paramount importance in order to ensure transparent, accountable, and trusted service providers. This is because the use of cloud services raises many compliance challenges [49].

5. Discussion

5.1 Summary of Results

Fig. 10 summarizes the key findings of the review with the first two columns showing the categorization based on the RQs. The third and fourth column of Fig. 10 presents the highly mentioned concepts and the evolving ones in the primary studies, respectively. With regard to industry requirements and user contexts, the security requirement is the top mentioned requirement for healthcare and finance with six mentions for each according to our analysis in Section 4.2. Similarly, the security requirement is also a top discussion in the context of end users with 30 mentions and developers with four mentions (Section 4.2). The highly mentioned theories and concepts are planned behavior, deterrence and requirement engineering, and evolving ones are workarounds, privacy by design and compliance by design as shown in second row of the Fig. 10 (Section 4.3.). The factors are divided based on their scope of impact as shown in the third row of Fig. 10. The highly mentioned factors are attitude towards compliance, subjective norms, and punishment, while the evolving one is the security stress (Section 4.3). Lastly, policies are categorized into three groups based on challenges they address (human, technological, and both) as shown in the last row of Fig. 10 in that SETA, software certification and regulation-driven architecture, and automation ranked as top most cited policies, with the concept of policy-as-code evolving (Section 4.4).

Journal Pre-proof



		Highly Cited	Evolving Concepts
15 Requirements *Section 4.2*	15 Industries	Healthcare: Security and Legal	
		Finance: Security and Auditing	
	11 User Context	End User: Security & Accessibility	
		Developers: Security, Safety and Legal	
Theories/Concepts *Section 4.3*	37 Theories	Planned Behavior	Workarounds
		Deterrence	
	35 Concepts	Requirement Engineering	Privacy-by-Design Compliance-by-Design
55 Factors *Section 4.3*	36 Individual	Attitude Towards Compliance	Security Stress
	7 Cultural	Subjective Norms	
	12 Organizational	Punishment	
19 Policies *Section 4.4*	10 Human-related	Security Education Training and Awareness	Policy-as-Code
	8 Technology-related	Certification & Regulation-driven Architecture	
	1 Human & Technology	Automation of Compliance Management	

Fig.10. Key Highlights of Top Cited and Evolving Concepts

Journal Pre-proof

The third column of Fig. 10 indicates that these topics are well explored in the field of software compliance. This level of attention gained for these topics represent their importance in the domain. This could either be for a certain industry, theories, impacting factors, or matured policies. On the other hand, the emerging concepts shown in the last column of Fig. 10 could indicate either growing types of compliance challenge, mechanisms to enhance compliance, or a factor gaining more attention.

5.2. Implications of Findings

5.2.1. Implications related to compliance requirements

Regarding compliance requirements, the following findings (F) represent major focus among the reviewed studies: First, security compliance (F1) is the top discussed topic in many industries (Fig.5 of Section 4.2), and it is highly associated with end users (Fig.6 of Section 4.2). It is also highlighted by many professional organizations and market research companies that end users are the most vulnerable to noncompliance and security breaches [1]. In addition to that, with the growing concerns of security attacks and breaches, research related to software security compliance of end users is expected to grow. Although end users gain more focus than other stakeholders like managers, developers, domain and legal experts which is typical since they are the ones dealing with information systems most frequently; and at the same time account for over 50% of security breaches, **the legal concerns of E-type software systems around end users still needs further investigation**. Second, legal and privacy requirements (F2) come next after security in that healthcare sector seems to place security, legal and privacy aspects as top priority, while security and licensing seem to be of a great deal in the software industry. The analysis indicates that peculiarities of each industry pose different priorities to certain requirements over others.

For example, apart from security being positioned as a high priority by most industries, licensing comes in the second priority for the software industry; and auditing is the second priority requirement for the financial industry. This entails each industry can prioritize its needed policies based on their requirements priorities; and in turn, **suggests more investigation for specific industries to be considered**. Third, from a software developer perspective, the security, safety, legal, licensing and architectural requirements (F3) are widely discussed topics (Fig.6 of Section 4.2). As software systems are a reflection of various requirements (functional and nonfunctional) and regulations (aka code is law), developers are in the forefront and considered the law enforcers. There is an emphasis found on the gap between developers, legal and compliance experts. Therefore, there is a need to **bridge this gap between domain and compliance experts on one side and software developers and engineers** on the other side. Research can also pay attention to other important stakeholders. These include software architects and engineers, who are the foremost concerned with the underlying design and development of software systems. Furthermore, compliance research around **business processes, usability, and accessibility in the context of software developers** remains insufficiently explored. Table 5 summarizes the key points of potential research recommendations.

5.2.2. Implications related to factors impacting compliance

With regard to factors impacting compliance, organizations should carefully look into individual and cultural aspects when designing compliance policy, since they contribute more to shaping compliance attitudes and behaviors within organizations (Fig.8 of Section 4.3). As our review found only a few studies addressing compliance attitudes, further research can investigate more factors that might influence compliance attitudes. With regard to identified factors, some of them were tested by more than one study, which increases the validity of their impact. However, most of the identified factors were tested by only one study, which makes it difficult to ensure validity of results and generalizability to all contexts and cultures. Peculiarities of a context are crucial, to spot critical factors and develop proper policies accordingly. Nevertheless, we identified factors, which are tested empirically in different contexts. In that, **decision makers should highly pay attention to the context**, since its impact on compliance has been confirmed and is likely generalizable to a greater extent. The critical factors that have a big impact on the overall compliance based on their scope of impact (individual, cultural, and organizational) are as follows: First, the majority of these factors focus on an individual's behavior and protection motivation. These are self-efficacy, attitude towards compliance, response efficacy, as well as perception of vulnerabilities and threads. Second, organizations should consider analyzing subjective, descriptive and social norms, since they are confirmed by several studies to play a nontrivial role in shaping compliance attitude and in turn behavior. Third, besides that, having a deterrence instrument in the form of punishment and sanctions should also be in place, in order to raise an individual's perception on the consequences of noncompliance. Concluding, no matter how well strategies and procedures are formulated by an organization, the **individual and cultural characteristics should not be ignored**. Otherwise, strategies will not be successful.

5.2.3. Implications related to theories

Previous research in the software compliance domain has focused on the individual characteristics as key factors and rationale behind a certain compliance behavior. This review shows that the highly dominant theories used by previous research are the theory of planned behavior [94], deterrence theory [105], and protection motivation theory [101], respectively. Other theories used are rational choice theory [106],

Journal Pre-proof

social bond theory [107], neutralization theory [98], organizational climate theory [108] and the theory of workarounds [109]. The latter is one of the growing theories used in the domain of shadow information systems and technical debts. It addresses the issue that the more complex the compliance measures are, the more likely to result in workarounds. Research on factors that leads to development of workarounds in information systems is growing.

As human users are the weakest link in the compliance chain, most of the reviewed studies pay more attention to the drivers that influence/deter individual behavior towards compliance/noncompliance. While most of the theories look into factors impacting compliance, what we see is missing based on previous research is testing the ultimate objective behind compliance or noncompliance. In this regard, the theory of reasoned goal pursuit [95] incorporates the concepts of procurement and active goals indicating the ultimate gain obtained out of performing a certain behavior, which none of the reviewed studies took into account. Considering such concepts in future research would add more value in understanding how the ultimate goals impact one's compliance behavior. Table 5 shows key recommendations for future research.

5.2.4. Implications related to software compliance policies

Our review also found that policies related to software compliance can be categorized into human-related policies and technology-related policies based on challenges they address (Table 3 of Section 4.4). Most of the surveyed policies (P) focus more on the human side of compliance than to the technological side. This could either indicate that compliance related to human behavior is largely addressed and compliance related to technological challenges neglected, or addressing human related policies might be easier to create than those related to technological ones. Based on the analysis of highly cited policies, we also found three major policies that contribute to addressing most of the compliance challenges. Automation of compliance management (P1, Sections 4.4.1.1 and 4.4.2.1) can address some of both human and technological challenges, in that less human involvement makes managing and checking compliance more effective and less error-prone. For example, misconfiguration of infrastructure or misinterpretation of requirements by different stakeholders happens very often once performed manually. Therefore, **organizations should consider automating compliance management** to avoid mistakes and misinterpretation resulting from manual checking. Organizations should also conduct security education, training and awareness (SETA) programs on a regular basis (P2), since they can help tackle many compliance challenges of an insider (Section 4.4.1.2). Another critical policy that organizations should pay attention to, is building organizational climate and social bonds (P3, Section 4.4.1.3). Having such a policy in place strengthens employees' attachment, commitment, involvement, and belief in organizational principle. This in turn strengthens the sense of belonging; and as a result, helps promote compliance culture and reduce negligence of insiders through influencing their compliance attitude. Other impactful policies discussed include deterrence instruments, reward and punishment, and internal auditing of workarounds. While there is no one size fits all when it comes to selection of appropriate policies that meet compliance needs. In other words, deciding the right policy mix varies according to business needs and alignment to corporate and industry requirements should be considered. A perfect policy recipe depends on the peculiarities of an organization and compliance challenges they need to address. Thus, practitioners should identify those peculiar needs and challenges when designing software related policies.

Policies related to technology are also of high importance to enhancing the overall compliance of software, as our analysis shows. Software certification practices and regulation driven architectures

Journal Pre-proof

should strongly be considered along with contemporary best practices (P4). Majority of the primary studies seem to not distinguish between open-source and proprietary software. **Making a distinction between open-source and proprietary** software is **important** though, since each might raise unique and different challenges, which have not been addressed by the reviewed articles. For example, license is more complicated in open source in that developers can end up using different components that may contradict in their underlying licensing agreement when it comes to use, derive or redistribute. On the other hand, software piracy is more common in proprietary software which is a big concern for end users. Similarly complication in other compliance requirements like security and legal could have different results having a clear distinction made between open source and proprietary software. In addition to that, it is critical to **support such policies with tools to provide a mechanism of enforcement and visibility to concerned stakeholders**, as also outlined in [110]. Having policies modeled in code can help avoid misinterpretation of these policies by stakeholders of different domains, while at the same time allow more automation and enforcement of compliance. The concept of policy as code has recently emerged in order to bridge this gap, but still in its infancy. Moreover, research related to software compliance modeling and supporting tools, which consider engaging concerned stakeholders throughout all stages of the software life cycle is understudied. This could be due to the difficulty arising from the fact that stakeholders of different domains use different vocabularies, methods and assumptions when analyzing and discussing issues related to software systems [64]. Furthermore, with the adoption of multiple devices and growing use of bring-your-own devices (BYOD) into workplaces, the consequences related to compliance management are likely to rise and can be threatening. While research on policies related BYOD still lacks sufficient investigation [16], studying compliance issues and challenges related to BYOD is worth exploring. Contrary to that, in a situation like the COVID-19 pandemic, many organizations respond to restrictions by allowing their employees to work from home and grant them access to organizational information systems and resources. This growing number of home users and the shift towards the home-office environment is expected to raise many compliance challenges including accessibility, security, privacy, and legal concerns and need to be addressed. Therefore, **future research can focus on policies and challenges related to home users**. The following Table 4 summarizes the key recommendations for future research.

Table 4. Summary of Further Research Recommendations

Requirements	1. Legal concerns of E-type software systems around end users needs further investigation.
	2. Research efforts should bridge the gap between domain & compliance experts and software developers.
	3. Further research should also study compliance of business processes, usability, and accessibility in the context of software developers.
Theories	1. As the theory of workarounds emerged, more research should explore antecedents of workarounds in compliance.
	2. The extended planned behavior, reasoned goal pursuit, helps understanding an individual’s goals that drive behaviors and, hence, deserves investigation.

Journal Pre-proof

Policies	1. Distinction between open source and proprietary software on compliance policies needs to be considered in future research.
	2. The lack of research on mechanisms for enforcement and visibility to concerned stakeholders should be resolved with further research.
	3. Research on policies related to home-office users deserve more attention.
	4. Since automation can address many compliance challenges, research efforts should consider development of supporting tools for enhancing automation of compliance.

6. Conclusion

6.1. Summary

In this article, we surveyed software compliance requirements, policies, and factors that impact different aspects of compliance by means of a systematic literature review. The systematic literature review methodology helps collecting and analyzing evidence from the state-of-the-art literature in a systematic and reproducible way. For our review, we enhanced the methodology developed by Kitchenham et al. [111] by introducing additional steps prior to deriving the research questions. These steps include surveying and analyzing existing reviews, in order to re-evaluate the review objective and derive the research questions. Using this methodology, we identified 77 primary articles that are relevant to addressing our review questions.

Our findings show that security concerns involving end users are the most often discussed compliance requirements. This is an expected result, since end users are responsible for over 50% of security breaches. Furthermore, concerns regarding privacy and accessibility are also growing. For software developers, security, safety, and legal aspects are the most relevant compliance requirements followed by licensing and architectural issues. While these results might seem obvious given that end users and developers are in the forefront and more concerned with these issues, the surveyed articles emphasize the gap between developers, legal, and compliance experts. The evolving concepts of privacy-by-design and compliance-by-design are expected to bridge this gap and enhance compliance management.

The factors that impact compliance are presented based on their scope of impact classified into individual, cultural, and organizational factors. Most of the identified factors are related to individual characteristics. One of the main issues in this regard is that users deliberately or inadvertently work around compliance requirements. This has led to the emergence of a new theory in the domain, namely the theory of workarounds.

The review also identified a list of policies and compliance challenges they address. Security education, training, and awareness should be a priority for every organization, since it helps mitigate the threat of insiders as the human factor is always the weakest link in the compliance chain. We also find that automation of compliance management tasks can help overcome challenges associated with manual compliance checking. This can be supported by the evolving concept of policy-as-code and help replace human involvement with more automation of compliance management. However, the lack of mechanisms and tools that provide enforcement and visibility to concerned stakeholders is yet a challenge. Promoting social bonds is another effective policy that is found to be effective in building attachment, commitment, involvement, and belief to corporate policies. This, in turn, reduces the negligence of insiders.

Journal Pre-proof

Journal Pre-proof

Surprisingly, there is no distinction made between open source and proprietary software when discussing compliance policies. Having such a distinction is important, since the two classes of software have different specifications for licensing, transparency, and legal requirements, which might generate some unique result for each.

The systematic literature review further presents implications and potential research directions with respect to these findings. Having insights on compliance requirements, policies, and factors and their impact, can empower practitioners and help them develop effective compliance strategies. Behavioral aspects dominate most of the compliance challenges, which indicate that no matter how sophisticated technological aspects are, the compliance at human side is challenging.

6.2. Limitations and Future Research

Although the review process and selection of articles has been conducted rigorously, we may have missed relevant studies that could have an impact on the findings and comprehensivity of this review.

In addition to that, the review focuses only on factors that directly influence various aspects of compliance but does not consider factors that have an indirect influence. It also needs to be noted that the results of some policies and factors were not tested in more than a single context (We indicated those studies in Section 4.1); based on the primary studies, which were selected according to the inclusion/exclusion criteria. In this regard, they might not be generalizable to all contexts. In such cases, additional tests might be needed to obtain more support for generalizability. Nevertheless, context peculiarities should also be considered.

Future research can further explore software compliance in the context of business processes, usability, and accessibility. Research can pay attention to other important stakeholders, as there is less focus on managers, engineers, domain and legal experts. Moreover, software architects and engineers, who are the people foremostly concerned with the design and the development of software systems, deserve more attention. Research efforts are also needed to help bridge the gap between domain and compliance experts on the one side and software developers and engineers on the other side.

While the theory of workarounds in the software compliance domain has been tested in the context of end users, there is a lack of research that tests the theory in the context of software engineers.

Besides that, the extended theory of planned behavior, reasoned goal pursuit, highlights the importance of considering the active goals as motivators towards a certain behavior. Although this can be crucial to compliance, none of the primary studies tested such a theory. Therefore, further studies can incorporate active procurement and approval goals when investigating the compliance behavior, in order to reveal more on the main triggers behind.

From a policy perspective, prioritization of policies is a challenge but could be based on the degree of impact. For instance, as an insider’s negligence accounts for 56% of software attacks, policies like SETA and organizational climate can be crucial for mitigating such an impact. While the difficulties of implementing these policies depend on compliance requirements and the context of applications, policies like automation of compliance and software certification might also require significant efforts to model the implementation. In this regard, a systematic review of case studies on policy implementation or even new case study research could help in evaluating the difficulties associated with implementation of policies and their pay off.

Journal Pre-proof

Acknowledgments:
This research was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. NRF-2022R1A2C1092077) and by the Global R&DB Program (IITP-2019-0-01328) supervised by the IITP (Institute for information & communications Technology Planning and Evaluation). Support came also from the Institute of Engineering Research at Seoul National University, which provided research facilities.

Declaration of Interest:
The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Declaration of interests

☒The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Journal Pre-proof

References

[1] PricewaterhouseCoopers, “Securing critical infrastructure: Get ready as voluntary becomes mandatory,” *PwC*, 2021. https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/biden-memo-signals-private-sector-cyber-performance-goals.html (accessed Jan. 09, 2022).

[2] Ponemon Institute, “2016 Cost of Data Center Outages,” *Ponemon Institute*, 2016. https://www.ponemon.org/research/ponemon-library/security/2016-cost-of-data-center-outages.html (accessed Jun. 19, 2022).

[3] Proofpoint, “2022 Ponemon Cost of Insider Threats Global Report,” 2022. https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-the-cost-of-insider-threats-ponemon-report.pdf (accessed Jun. 11, 2022).

[4] N. Guhr, B. Lebek, and M. H. Breitner, “The impact of leadership on employees’ intended information security behaviour: An examination of the full-range leadership theory,” *Information Systems Journal*, vol. 29, no. 2, pp. 340–362, 2019, doi: 10.1111/isj.12202.

[5] P. Balozian and D. Leidner, “Review of IS Security Policy Compliance: Toward the Building Blocks of an IS Security Theory,” *SIGMIS Database*, vol. 48, no. 3, pp. 11–43, Aug. 2017, doi: 10.1145/3130515.3130518.

[6] PWC, “the-global-state-of-information-security-survey-2015.pdf,” 2015. Accessed: Sep. 22, 2022. [Online]. Available: https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf

[7] PricewaterhouseCoopers, “Global State of Information Security® Survey 2018,” *PwC*, 2018. https://www.pwc.co.uk/issues/cyber-security-services/insights/global-state-of-information-security-survey.html (accessed Jan. 11, 2022).

[8] W. A. Cram, J. G. Proudfoot, and J. D’Arcy, “Organizational information security policies: a review and research framework,” *null*, vol. 26, no. 6, pp. 605–641, Nov. 2017, doi: 10.1057/s41303-017-0059-9.

[9] S. Trang and B. Brendel, “A Meta-Analysis of Deterrence Theory in Information Security Policy Compliance Research,” *Inf Syst Front*, vol. 21, no. 6, pp. 1265–1284, Dec. 2019, doi: 10.1007/s10796-019-09956-4.

Journal Pre-proof

[10] G. D. Moody, M. Siponen, and S. Pahnila, “Toward a Unified Model of Information Security Policy Compliance,” *MIS Quarterly*, vol. 42, no. 1, pp. 285-A22, Mar. 2018.

[11] P. Puhakainen and M. Siponen, “Improving Employees’ Compliance Through Information Systems Security Training: An Action Research Study,” *MIS Quarterly*, vol. 34, no. 4, pp. 757–778, 2010, doi: 10.2307/25750704.

[12] M. L. Hale and R. F. Gamble, “Semantic hierarchies for extracting, modeling, and connecting compliance requirements in information security control standards,” *Requirements Eng*, vol. 24, no. 3, pp. 365–402, Sep. 2019, doi: 10.1007/s00766-017-0287-5.

[13] R. F. Ali, P. D. D. Dominic, S. E. A. Ali, M. Rehman, and A. Sohail, “Information Security Behavior and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance,” *Applied Sciences*, vol. 11, no. 8, Art. no. 8, Jan. 2021, doi: 10.3390/app11083383.

[14] J. D’Arcy and T. Herath, “A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings,” *European Journal of Information Systems*, vol. 20, no. 6, pp. 643–658, Nov. 2011, doi: 10.1057/ejis.2011.23.

[15] S. Hina and P. D. D. Dominic, “Information security policies’ compliance: a perspective for higher education institutions,” *Journal of Computer Information Systems*, vol. 60, no. 3, pp. 201–211, May 2020, doi: 10.1080/08874417.2018.1432996.

[16] R. Palanisamy, A. A. Norman, and M. L. Mat Kiah, “BYOD Policy Compliance: Risks and Strategies in Organizations,” *null*, pp. 1–12, Feb. 2020, doi: 10.1080/08874417.2019.1703225.

[17] A. Tsohou and P. Holtkamp, “Are users competent to comply with information security policies? An analysis of professional competence models,” *Information Technology &amp; People*, Jul. 2018, doi: 10.1108/ITP-02-2017-0052.

[18] Z. Zandesh, M. Ghazisaeedi, M. V. Devarakonda, and M. S. Haghighi, “Legal framework for health cloud: A systematic review,” *International Journal of Medical Informatics*, vol. 132, p. 103953, Dec. 2019, doi: 10.1016/j.ijmedinf.2019.103953.

[19] B. A. Kitchenham, D. Budgen, P. Brereton, D. Budgen, and P. Brereton, *Evidence-Based Software Engineering and Systematic Reviews*. Chapman and Hall/CRC, 2016. doi: 10.1201/b19467.

[20] N. J. van Eck and L. Waltman, “VOSviewer Manual,” p. 51, 2018.

[21] J. P. Castellanos-Ardila, B. Gallina, and G. Governatori, “Compliance-aware engineering process plans: the case of space software engineering processes,” *Artif Intell Law*, Mar. 2021, doi: 10.1007/s10506-021-09285-5.

[22] C. Máñez-Carvajal, J. F. Cervera-Mérida, and R. Fernández-Piqueras, “Web accessibility evaluation of top-ranking university Web sites in Spain, Chile and Mexico,” *Univ Access Inf Soc*, vol. 20, no. 1, pp. 179–184, Mar. 2021, doi: 10.1007/s10209-019-00702-w.

[23] V. Diamantopoulou and H. Mouratidis, “Practical evaluation of a reference architecture for the management of privacy level agreements,” *Information & Computer Security*, vol. 27, no. 5, pp. 711–730, Jan. 2019, doi: 10.1108/ICS-04-2019-0052.

[24] T. Granlund, T. Mikkonen, and V. Stirbu, “On Medical Device Software CE Compliance and Conformity Assessment,” in *2020 IEEE International Conference on Software Architecture Companion (ICSA-C)*, Mar. 2020, pp. 185–191. doi: 10.1109/ICSA-C50368.2020.00040.

[25] M. Karjalainen, M. Siponen, P. Puhakainen, and S. Sarker, “Universal and Culture-dependent Employee Compliance of Information Systems Security Procedures,” *Journal of Global Information Technology Management*, vol. 23, no. 1, pp. 5–24, Jan. 2020, doi: 10.1080/1097198X.2019.1701355.

[26] K. Dong, R. F. Ali, P. D. D. Dominic, and S. E. A. Ali, “The Effect of Organizational Information Security Climate on Information Security Policy Compliance: The Mediating

Effect of Social Bonding towards Healthcare Nurses," *Sustainability*, vol. 13, no. 5, Art. no. 5, Jan. 2021, doi: 10.3390/su13052800.

[27] N. Humaidi and V. Balakrishnan, "Indirect effect of management support on users' compliance behaviour towards information security policies:," *Health Information Management Journal*, Mar. 2017, doi: 10.1177/1833358317700255.

[28] F. Karlsson, K. Hedström, and G. Goldkuhl, "Practice-based discourse analysis of information security policies," *Computers & Security*, vol. 67, pp. 267–279, Jun. 2017, doi: 10.1016/j.cose.2016.12.012.

[29] E. Kolkowska, F. Karlsson, and K. Hedström, "Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method," *The Journal of Strategic Information Systems*, vol. 26, no. 1, pp. 39–57, Mar. 2017, doi: 10.1016/j.jsis.2016.08.005.

[30] K.-M. Kuo, P. C. Talley, and D.-Y. M. Lin, "Hospital Staff's Adherence to Information Security Policy: A Quest for the Antecedents of Deterrence Variables," *INQUIRY*, vol. 58, p. 00469580211029599, Jan. 2021, doi: 10.1177/00469580211029599.

[31] S. T. Alanazi, M. Anbar, S. A. Ebad, S. Karuppayah, and H. A. Al-Ani, "Theory-Based Model and Prediction Analysis of Information Security Compliance Behavior in the Saudi Healthcare Sector," *Symmetry*, vol. 12, no. 9, Art. no. 9, Sep. 2020, doi: 10.3390/sym12091544.

[32] G. Carmi and D. Bouhnik, "The Effect of Rational Based Beliefs and Awareness on Employee Compliance with Information Security Procedures: A Case Study of a Financial Corporation in Israel," *Interdisciplinary Journal of Information, Knowledge, and Management*, vol. 15, pp. 109–125, Jul. 2020.

[33] Y. Chen, K. Ramamurthy, and K.-W. Wen, "Organizations' Information Security Policy Compliance: Stick or Carrot Approach?," *Journal of Management Information Systems*, vol. 29, no. 3, pp. 157–188, Dec. 2012, doi: 10.2753/MIS0742-1222290305.

[34] S. Jeon, I. Son, and J. Han, "Exploring the role of intrinsic motivation in ISSP compliance: enterprise digital rights management system case," *Information Technology & People*, vol. 34, no. 2, pp. 599–616, Jan. 2020, doi: 10.1108/ITP-05-2018-0256.

[35] M. I. Merhi and P. Ahluwalia, "Examining the impact of deterrence factors and norms on resistance to Information Systems Security," *Computers in Human Behavior*, vol. 92, pp. 37–46, Mar. 2019, doi: 10.1016/j.chb.2018.10.031.

[36] K. Rongrat and T. Senivongse, "Assessing Risk of Security Non-compliance of Banking Security Requirements Based on Attack Patterns," *International Journal of Networked and Distributed Computing*, vol. 6, no. 1, pp. 1–10, Jan. 2018, doi: 10.2991/ijndc.2018.6.1.1.

[37] J. C. Westland, "The information content of Sarbanes-Oxley in predicting security breaches," *Computers & Security*, vol. 90, p. 101687, Mar. 2020, doi: 10.1016/j.cose.2019.101687.

[38] G. Bansal, S. Muzatko, and S. I. Shin, "Information system security policy noncompliance: the role of situation-specific ethical orientation," *Information Technology & People*, vol. 34, no. 1, pp. 250–296, Jan. 2020, doi: 10.1108/ITP-03-2019-0109.

[39] X. Chen, D. Wu, L. Chen, and J. K. L. Teng, "Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and control variables," *Information & Management*, vol. 55, no. 8, pp. 1049–1060, Dec. 2018, doi: 10.1016/j.im.2018.05.011.

[40] S. Hina, D. D. D. Panneer Selvam, and P. B. Lowry, "Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world," *Computers & Security*, vol. 87, p. 101594, Nov. 2019, doi: 10.1016/j.cose.2019.101594.

[41] I. Wiafe, F. N. Koranteng, A. Wiafe, E. N. Obeng, and W. Yaokumah, "The role of norms

Journal Pre-proof

in information security policy compliance," *Information &amp; Computer Security*, Jun. 2020, doi: 10.1108/ICS-08-2019-0095.

[42] S. Thalmann, D. Bachlechner, L. Demetz, and M. Manhart, "Complexity is dead, long live complexity! How software can help service providers manage security and compliance," *Computers & Security*, vol. 45, pp. 172–185, Sep. 2014, doi: 10.1016/j.cose.2014.05.012.

[43] N.-T. Truong and V.-H. Nguyen, "An approach to checking the compliance of user permission policy in software development," *Int. J. Soft. Eng. Knowl. Eng.*, vol. 23, no. 08, pp. 1139–1151, Oct. 2013, doi: 10.1142/S0218194013500344.

[44] Á. J. Varela-Vaca, R. M. Gasca, R. Ceballos, M. T. Gómez-López, and P. B. Torres, "CyberSPL: A Framework for the Verification of Cybersecurity Policy Compliance of System Configurations Using Software Product Lines," *Applied Sciences*, vol. 9, no. 24, Art. no. 24, Jan. 2019, doi: 10.3390/app9245364.

[45] M. Choi and J. Song, "Social control through deterrence on the compliance with information security policy," *Soft Comput*, vol. 22, no. 20, pp. 6765–6772, Oct. 2018, doi: 10.1007/s00500-018-3354-z.

[46] C. Liu, C. Wang, H. Wang, and B. Niu, "Influencing factors of employees' information systems security police compliance: An empirical research in China," in *E3S Web of Conferences*, Les Ulis, France, 2020, vol. 218. doi: http://dx.doi.org/10.1051/e3sconf/202021804032.

[47] R. F. Ali, P. D. D. Dominic, and K. Ali, "Organizational Governance, Social Bonds and Information Security Policy Compliance: A Perspective towards Oil and Gas Employees," *Sustainability*, vol. 12, no. 20, Art. no. 20, Jan. 2020, doi: 10.3390/su12208576.

[48] S. S. Kim and Y. J. Kim, "The effect of compliance knowledge and compliance support systems on information security compliance behavior," *Journal of Knowledge Management*, vol. 21, no. 4, pp. 986–1010, Jan. 2017, doi: 10.1108/JKM-08-2016-0353.

[49] S. Majumdar *et al.*, "User-Level Runtime Security Auditing for the Cloud," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 5, pp. 1185–1199, May 2018, doi: 10.1109/TIFS.2017.2779444.

[50] S. Ingolfo, A. Siena, J. Mylopoulos, A. Susi, and A. Perini, "Arguing regulatory compliance of software requirements," *Data & Knowledge Engineering*, vol. 87, pp. 279–296, Sep. 2013, doi: 10.1016/j.datak.2012.12.004.

[51] P. Li *et al.*, "ChainSDI: A Software-Defined Infrastructure for Regulation-Compliant Home-Based Healthcare Services Secured by Blockchains," *IEEE Systems Journal*, vol. 14, no. 2, pp. 2042–2053, Jun. 2020, doi: 10.1109/JSYST.2019.2937930.

[52] J. C. Maxwell, A. I. Antón, P. Swire, M. Riaz, and C. M. McCraw, "A legal cross-references taxonomy for reasoning about compliance requirements," *Requirements Eng*, vol. 17, no. 2, pp. 99–115, 2013, doi: 10.1007/s00766-012-0152-5.

[53] A. A. Mohamed, N. El-bendary, and A. Abdo, "Law Architecture for Regulatory-Compliant Public Enterprise Model: A Focus on Healthcare Reform in Egypt," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 12, no. 6, Art. no. 6, 30 2021, doi: 10.14569/IJACSA.2021.0120638.

[54] M. A. Islam, M. A. Khan, A. Z. M. Obaidullah, and M. S. Alam, "Effect of entrepreneur and firm characteristics on the business success of small and medium enterprises (SMEs) in Bangladesh," *International Journal of Business and Management*, vol. 6, no. 3, p. 289, 2011.

[55] K. P. Joshi, L. Elluri, and A. Nagar, "An Integrated Knowledge Graph to Automate Cloud Data Compliance," *IEEE Access*, vol. 8, pp. 148541–148555, 2020, doi: 10.1109/ACCESS.2020.3008964.

[56] M. Usman, M. Felderer, M. Unterkalmsteiner, E. Klotins, D. Mendez, and E. Alégroth, "Compliance Requirements in Large-Scale Software Development: An Industrial Case Study," in *Product-Focused Software Process Improvement*, Cham, 2020, pp. 385–401.

Journal Pre-proof

doi: 10.1007/978-3-030-64148-1_24.

[57] B. Eze, C. Kuziemsky, and L. Peyton, “Operationalizing Privacy Compliance for Cloud-Hosted Sharing of Healthcare Data,” in *2018 IEEE/ACM International Workshop on Software Engineering in Healthcare Systems (SEHS)*, May 2018, pp. 18–25.

[58] R. Samavi and M. P. Consens, “Publishing privacy logs to facilitate transparency and accountability,” *Journal of Web Semantics*, vol. 50, pp. 1–20, May 2018, doi: 10.1016/j.websem.2018.02.001.

[59] T. Antignac, R. Scandariato, and G. Schneider, “Privacy Compliance Via Model Transformations,” in *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*, Apr. 2018, pp. 120–126. doi: 10.1109/EuroSPW.2018.00024.

[60] K. Bednar, S. Spiekermann, and M. Langheinrich, “Engineering Privacy by Design: Are engineers ready to live up to the challenge?,” *The Information Society*, vol. 35, no. 3, pp. 122–142, May 2019, doi: 10.1080/01972243.2019.1583296.

[61] G. R. Gangadharan, V. D’Andrea, S. De Paoli, and M. Weiss, “Managing license compliance in free and open source software development,” *Inf Syst Front*, vol. 14, no. 2, pp. 143–154, Apr. 2012, doi: 10.1007/s10796-009-9180-1.

[62] R. Moquin and R. L. Wakefield, “The Roles of Awareness, Sanctions, and Ethics in Software Compliance,” *Journal of Computer Information Systems*, vol. 56, no. 3, pp. 261–270, Jul. 2016, doi: 10.1080/08874417.2016.1153922.

[63] M. Sojer, O. Alexy, S. Kleinknecht, and J. Henkel, “Understanding the Drivers of Unethical Programming Behavior: The Inappropriate Reuse of Internet-Accessible Code,” *Journal of Management Information Systems*, vol. 31, no. 3, pp. 287–325, Jul. 2014, doi: 10.1080/07421222.2014.995563.

[64] K. Julisch, C. Suter, T. Woitalla, and O. Zimmermann, “Compliance by design – Bridging the chasm between auditors and IT architects,” *Computers & Security*, vol. 30, no. 6, pp. 410–426, Sep. 2011, doi: 10.1016/j.cose.2011.03.005.

[65] C. Wickramage, C. Fidge, C. Ouyang, and T. Sahama, “Generating Log Requirements for Checking Conformance against Healthcare Standards Using Workflow Modelling,” New York, NY, USA, 2019. doi: 10.1145/3290688.3290739.

[66] J. Marques and A. M. da Cunha, “Tailoring Traditional Software Life Cycles to Ensure Compliance of RTCA DO-178C and DO-331 with Model-Driven Design,” in *2018 IEEE/AIAA 37th Digital Avionics Systems Conference (DASC)*, Sep. 2018, pp. 1–8. doi: 10.1109/DASC.2018.8569351.

[67] V. Antinyan and H. Sandgren, “Software Safety Analysis to Support ISO 26262-6 Compliance in Agile Development,” *IEEE Software*, vol. 38, no. 3, pp. 52–60, May 2021, doi: 10.1109/MS.2020.3026145.

[68] K. Chitnis *et al.*, “Enabling Functional Safety ASIL Compliance for Autonomous Driving Software Systems,” *Electronic Imaging*, vol. 2017, no. 19, pp. 35–40, Jan. 2017, doi: 10.2352/ISSN.2470-1173.2017.19.AVM-017.

[69] A. C. Oliveira, L. F. da Silva, M. M. Eler, and A. P. Freire, “Do Brazilian Federal Agencies Specify Accessibility Requirements for the Development of their Mobile Apps?,” in *XVI Brazilian Symposium on Information Systems*, São Bernardo do Campo Brazil, Nov. 2020, pp. 1–8. doi: 10.1145/3411564.3411643.

[70] M. Montazeri, R. Khajouei, and M. Montazeri, “Evaluating hospital information system according to ISO 9241 part 12,” *Digit. Health*, vol. 6, p. 2055207620979466, Dec. 2020, doi: 10.1177/2055207620979466.

[71] P. Balozian, D. Leidner, and B. Xue, “Toward an intellectual capital cyber security theory: insights from Lebanon,” *Journal of Intellectual Capital*, vol. ahead-of-print, no. ahead-of-print, Art. no. ahead-of-print, Jan. 2021, doi: 10.1108/JIC-05-2021-0123.

[72] A. J. Burns, T. L. Roberts, C. Posey, R. J. Bennett, and J. F. Courtney, “Intentions to Comply Versus Intentions to Protect: A VIE Theory Approach to Understanding the

Journal Pre-proof

Influence of Insiders' Awareness of Organizational SETA Efforts," *Decision Sciences*, vol. 49, no. 6, pp. 1187–1228, 2018, doi: 10.1111/deci.12304.

[73] J. D'Arcy, T. Herath, and M. K. Shoss, "Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective," *Journal of Management Information Systems*, vol. 31, no. 2, pp. 285–318, Oct. 2014, doi: 10.2753/MIS0742-1222310210.

[74] S. M. Faizi and S. S. M. Rahman, "Effect of Fear on Behavioral Intention to Comply," in *Proceedings of the 2020 the 4th International Conference on Information System and Data Mining*, New York, NY, USA, May 2020, pp. 65–70. doi: 10.1145/3404663.3404685.

[75] B. Guan and C. Hsu, "The role of abusive supervision and organizational commitment on employees' information security policy noncompliance intention," *Internet Research*, vol. 30, no. 5, pp. 1383–1405, Jan. 2020, doi: 10.1108/INTR-06-2019-0260.

[76] C. Liu, N. Wang, and H. Liang, "Motivating information security policy compliance: The critical role of supervisor-subordinate guanxi and organizational commitment," *International Journal of Information Management*, vol. 54, p. 102152, Oct. 2020, doi: 10.1016/j.ijinfomgt.2020.102152.

[77] D. Ormond, M. Warkentin, and R. E. Crossler, "Integrating Cognition with an Affective Lens to Better Understand Information Security Policy Compliance," *Journal of the Association for Information Systems*, vol. 20, no. 12, pp. 1794–1843, Dec. 2019, doi: 10.17705/1jais.00586.

[78] F. Putri and A. Hovav, "Employees' compliance with BYOD security policy: Insights from reactance, organizational justice, and protection motivation theory," presented at the ECIS 2014 Proceedings - 22nd European Conference on Information Systems, 2014.

[79] T. Stafford, G. Deitz, and Y. Li, "The role of internal audit and user training in information security policy compliance," *Managerial Auditing Journal*, vol. 33, no. 4, pp. 410–424, Jan. 2018, doi: 10.1108/MAJ-07-2017-1596.

[80] C. Van Slyke and F. Belanger, "Explaining the interactions of humans and artifacts in insider security behaviors: The mangle of practice perspective," *Computers & Security*, vol. 99, p. 102064, Dec. 2020, doi: 10.1016/j.cose.2020.102064.

[81] M. Barati, O. Rana, I. Petri, and G. Theodorakopoulos, "GDPR Compliance Verification in Internet of Things," *IEEE Access*, vol. 8, pp. 119697–119709, 2020, doi: 10.1109/ACCESS.2020.3005509.

[82] R. Davison, L. H. Wong, S. Alter, and C. Ou, "Adopted globally but unusable locally: what workarounds reveal about adoption, resistance, compliance and non-compliance," May 2019. [Online]. Available: https://aisel.aisnet.org/ecis2019_rp/19

[83] C. Czepa, H. Tran, U. Zdun, T. T. T. Kim, E. Weiss, and C. Ruhsam, "On the Understandability of Semantic Constraints for Behavioral Software Architecture Compliance: A Controlled Experiment," in *2017 IEEE International Conference on Software Architecture (ICSA)*, Apr. 2017, pp. 155–164. doi: 10.1109/ICSA.2017.10.

[84] E. Silva, T. Batista, and F. Oquendo, "On the verification of mission-related properties in software-intensive systems-of-systems architectural design," *Science of Computer Programming*, vol. 192, p. 102425, Jun. 2020, doi: 10.1016/j.scico.2020.102425.

[85] K. Singi, J. C. B. R P, S. Podder, and A. P. Burden, "Trusted Software Supply Chain," in *2019 34th IEEE/ACM International Conference on Automated Software Engineering (ASE)*, Nov. 2019, pp. 1212–1213. doi: 10.1109/ASE.2019.00141.

[86] P. Ifinedo, "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory," *Computers & Security*, vol. 31, no. 1, pp. 83–95, Feb. 2012, doi: 10.1016/j.cose.2011.10.007.

[87] P. Ifinedo, "Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition," *Information & Management*, vol. 51, no. 1, Art. no. 1, Jan. 2014, doi: 10.1016/j.im.2013.10.001.

Journal Pre-proof

Journal Pre-proof

[88] P. Ifinedo, “Critical Times for Organizations: What Should Be Done to Curb Workers’ Noncompliance With IS Security Policy Guidelines?,” *Information Systems Management*, vol. 33, no. 1, pp. 30–41, Jan. 2016, doi: 10.1080/10580530.2015.1117868.

[89] A. Steffens, H. Lichter, and M. Moscher, “Towards data-driven continuous compliance testing,” 2018, vol. 2066, pp. 78–84.

[90] S. H. Kim, K. H. Yang, and S. Park, “An Integrative Behavioral Model of Information Security Policy Compliance,” *The Scientific World Journal*, vol. 2014, p. e463870, May 2014, doi: 10.1155/2014/463870.

[91] S. Alter, “Beneficial noncompliance and detrimental compliance: Expected paths to unintended consequences,” presented at the 2015 Americas Conference on Information Systems, AMCIS 2015, 2015.

[92] M. Siponen, M. Adam Mahmood, and S. Pahnila, “Employees’ adherence to information security policies: An exploratory field study,” *Information & Management*, vol. 51, no. 2, pp. 217–224, Mar. 2014, doi: 10.1016/j.im.2013.08.006.

[93] T.-B. Lembcke, K. Masuch, S. Trang, S. Hengstler, P. Plics, and M. Pamuk, “Fostering Information Security Compliance: Comparing the Predictive Power of Social Learning Theory and Deterrence Theory,” *AMCIS 2019 Proceedings*, Jul. 2019, [Online]. Available: https://aisel.aisnet.org/amcis2019/info_security_privacy/info_security_privacy/26

[94] I. Ajzen, “The theory of planned behavior,” *Organizational Behavior and Human Decision Processes*, vol. 50, no. 2, pp. 179–211, Dec. 1991, doi: 10.1016/0749-5978(91)90020-T.

[95] I. Ajzen and A. W. Kruglanski, “Reasoned action in the service of goal pursuit,” *Psychological Review*, vol. 126, no. 5, pp. 774–786, Oct. 2019, doi: 10.1037/rev0000155.

[96] N. T. Feather, “Values, valences, and choice: The influences of values on the perceived attractiveness and choice of alternatives,” *Journal of Personality and Social Psychology*, vol. 68, no. 6, pp. 1135–1151, 1995, doi: 10.1037/0022-3514.68.6.1135.

[97] T. S. Ragu-Nathan, M. Tarafdar, B. S. Ragu-Nathan, and Q. Tu, “The Consequences of Technostress for End Users in Organizations: Conceptual Development and Empirical Validation,” *Information Systems Research*, vol. 19, no. 4, pp. 417–433, Dec. 2008, doi: 10.1287/isre.1070.0165.

[98] G. M. Sykes and D. Matza, “Techniques of Neutralization: A Theory of Delinquency,” *American Sociological Review*, vol. 22, no. 6, pp. 664–670, 1957, doi: 10.2307/2089195.

[99] T. Herath and H. R. Rao, “Protection motivation and deterrence: a framework for security policy compliance in organisations,” *Eur J Inf Syst*, vol. 18, no. 2, pp. 106–125, Apr. 2009, doi: 10.1057/ejis.2009.6.

[100] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, “Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness,” *MIS Quarterly*, vol. 34, no. 3, pp. 523–548, 2010, doi: 10.2307/25750690.

[101] R. W. Rogers and S. Prentice-Dunn, “Protection motivation theory,” in *Handbook of health behavior research 1: Personal and social determinants*, New York, NY, US: Plenum Press, 1997, pp. 113–132.

[102] M. Fishbein and I. Ajzen, *Predicting and Changing Behavior: The Reasoned Action Approach*. New York: Psychology Press, 2009. doi: 10.4324/9780203838020.

[103] H. Tran, U. Zdun, T. Holmes, E. Oberortner, E. Mulo, and S. Dustdar, “Compliance in service-oriented architectures: A model-driven and view-based approach,” *Information and Software Technology*, vol. 54, no. 6, pp. 531–552, Jun. 2012, doi: 10.1016/j.infsof.2012.01.001.

[104] M. M. Lehman, “Programs, life cycles, and laws of software evolution,” *Proceedings of the IEEE*, vol. 68, no. 9, pp. 1060–1076, Sep. 1980, doi: 10.1109/PROC.1980.11805.

[105] R. Jervis, “Deterrence Theory Revisited,” *World Politics*, vol. 31, no. 2, pp. 289–324, Jan. 1979, doi: 10.2307/2009945.

[106] J. Scott, “Rational Choice Theory,” in *Understanding Contemporary Society: Theories of*

Journal Pre-proof

Journal Pre-proof

the Present, London: SAGE Publications Ltd, 2000, pp. 126–138. doi: 10.4135/9781446218310.

[107] T. Hirschi and R. Stark, “Hellfire and Delinquency*,” *Social Problems*, vol. 17, no. 2, pp. 202–213, Oct. 1969, doi: 10.2307/799866.

[108] B. Schneider, A. P. Brief, and R. A. Guzzo, “Creating a climate and culture for sustainable organizational change,” *Organizational Dynamics*, vol. 24, no. 4, pp. 7–19, Mar. 1996, doi: 10.1016/S0090-2616(96)90010-8.

[109] S. Alter, “Theory of Workarounds,” *Business Analytics and Information Systems*, Mar. 2014, [Online]. Available: https://repository.usfca.edu/at/40

[110] M. Mubarkoot and J. Altmann, “Towards Software Compliance Specification and Enforcement Using TOSCA,” in *Economics of Grids, Clouds, Systems, and Services*, Sep. 2021, pp. 168–177. doi: 10.1007/978-3-030-92916-9_14.

[111] B. A. Kitchenham, D. Budgen, P. Brereton, D. Budgen, and P. Brereton, *Evidence-Based Software Engineering and Systematic Reviews*. Chapman and Hall/CRC, 2016. doi: 10.1201/b19467.

[112] H. Weiss and R. Cropanzano, “Affective Events Theory,” *Research in organizational behavior*, vol. 18, pp. 1--74, 1966.

[113] M. Fishbein, “A theory of reasoned action: Some applications and implications,” *Nebraska Symposium on Motivation*, vol. 27, pp. 65–116, 1979.

[114] E. L. Deci and R. M. Ryan, “Cognitive Evaluation Theory,” in *Intrinsic Motivation and Self-Determination in Human Behavior*, E. L. Deci and R. M. Ryan, Eds. Boston, MA: Springer US, 1985, pp. 43–85. doi: 10.1007/978-1-4899-2271-7_3.

[115] L. Kohlberg, “The Psychology of Moral Development,” *Ethics*, vol. 97, no. 2, pp. 441–456, 1987, doi: 10.1086/292850.

[116] A. Bandura, “Social Cognitive Theory of Moral Thought and Action,” in *Handbook of Moral Behavior and Development*, Psychology Press, 1991.

[117] R. S. Lazarus and S. Folkman, *Stress, Appraisal, and Coping*. Springer Publishing Company, 1984.

[118] J. Potter and M. Wetherell, *Discourse and social psychology: Beyond attitudes and behaviour*. Sage, 1987.

[119] T. M. Jones, “Ethical Decision Making by Individuals in Organizations: An Issue-Contingent Model,” *AMR*, vol. 16, no. 2, pp. 366–395, Apr. 1991, doi: 10.5465/amr.1991.4278958.

[120] B. Victor and J. B. Cullen, “The Organizational Bases of Ethical Work Climates,” *Administrative Science Quarterly*, vol. 33, no. 1, pp. 101–125, 1988, doi: 10.2307/2392857.

[121] P. J. H. Schoemaker, “The Expected Utility Model: Its Variants, Purposes, Evidence and Limitations,” *Journal of Economic Literature*, vol. 20, no. 2, pp. 529–563, 1982.

[122] G. De Sanctis, “Expectancy Theory as an Explanation of Voluntary Use of a Decision-Support System,” *Psychol Rep*, vol. 52, no. 1, pp. 247–260, Feb. 1983, doi: 10.2466/pr0.1983.52.1.247.

[123] A. Pickering, “The Mangle of Practice: Agency and Emergence in the Sociology of Science,” *American Journal of Sociology*, vol. 99, no. 3, pp. 559–589, Nov. 1993, doi: 10.1086/230316.

[124] J. W. Brehm, *A theory of psychological reactance*. Oxford, England: Academic Press, 1966, pp. x, 135.

[125] J. G. Sutinen and K. Kuperan, “A socio- economic theory of regulatory compliance,” *International Journal of Social Economics*, vol. 26, no. 1/2/3, pp. 174–193, Jan. 1999, doi: 10.1108/03068299910229569.

[126] E. L. Deci, H. Eghrari, B. C. Patrick, and D. R. Leone, “Facilitating Internalization: The Self-Determination Theory Perspective,” *Journal of Personality*, vol. 62, no. 1, pp. 119–

Journal Pre-proof

142, 1994, doi: 10.1111/j.1467-6494.1994.tb00797.x.

[127] R. P. Settoon, N. Bennett, and R. C. Liden, “Social exchange in organizations: Perceived organizational support, leader–member exchange, and employee reciprocity,” *Journal of Applied Psychology*, vol. 81, pp. 219–227, 1996, doi: 10.1037/0021-9010.81.3.219.

[128] H. Liang and Y. (Lucky) Xue, “Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective,” *Journal of the Association for Information Systems*, vol. 11, no. 7, Jul. 2010, doi: 10.17705/1jais.00232.

[129] R. L. Akers, M. D. Krohn, L. Lanza-Kaduce, and M. Radosevich, “Social Learning and Deviant Behavior: A Specific Test of a General Theory,” in *Contemporary Masters in Criminology*, J. McCord and J. H. Laub, Eds. Boston, MA: Springer US, 1995, pp. 187–214. doi: 10.1007/978-1-4757-9829-6_12.

[130] D. C. Hambrick and P. A. Mason, “Upper Echelons: The Organization as a Reflection of Its Top Managers,” *AMR*, vol. 9, no. 2, pp. 193–206, Apr. 1984, doi: 10.5465/amr.1984.4277628.

[131] I. Niiniluoto, *Critical Scientific Realism*. OUP Oxford, 1999.

[132] K. Hedström, E. Kolkowska, F. Karlsson, and J. P. Allen, “Value conflicts for information security management,” *The Journal of Strategic Information Systems*, vol. 20, no. 4, pp. 373–384, Dec. 2011, doi: 10.1016/j.jsis.2011.06.001.

[133] S. Alter, “Work System Theory: Overview of Core Concepts, Extensions, and Challenges for the Future,” *Journal of the Association for Information Systems*, pp. 72–121, Feb. 2013.

Appendices:

Appendix A. Scholarly databases and corresponding search queries used for each database to retrieve articles.

Scholarly Database	Search Query
Google Scholar (Titles Only)	software compliance; compliance "information systems"; compliance "distributed systems"; compliance "software systems"; compliance "service-oriented systems"
Web of Science	("software compliance" OR "compliance of software" OR (compliance AND "information systems") OR (compliance AND "distributed systems") OR (compliance AND "software systems") OR (compliance AND "service-oriented systems"))
ScienceDirect	"software compliance" OR "compliance of software" OR (compliance AND "information systems") OR (compliance AND "distributed systems") OR (compliance AND "software systems") OR (compliance AND "service-oriented systems")
Scopus	("software *compliance" OR "*compliance of software" OR (*compliance AND "information system*") OR (*compliance AND "distributed system*") OR (*compliance AND "software system*") OR (*compliance AND "service-oriented system*"))

Journal Pre-proof

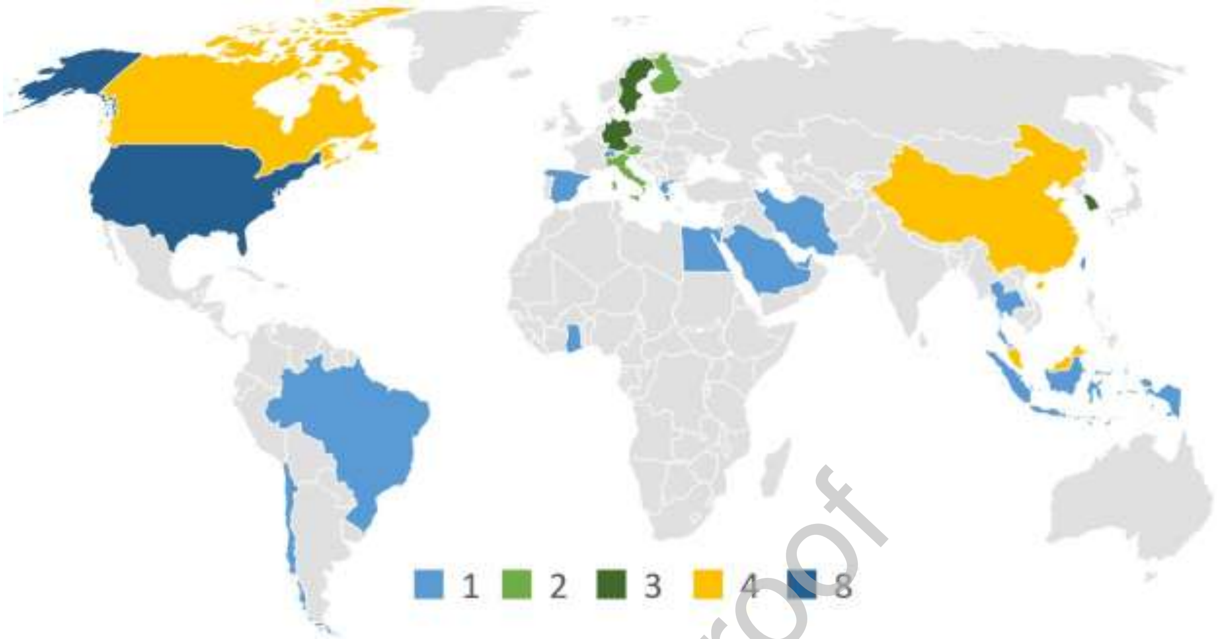
ACM Digital Library	("software compliance" OR "compliance of software" OR (compliance AND "information systems") OR (compliance AND "distributed systems") OR (compliance AND "software systems") OR (compliance AND "service-oriented systems"))
IEEE Xplore	"software compliance" OR "compliance of software" OR (compliance AND "information systems") OR (compliance AND "distributed systems") OR (compliance AND "software systems") OR (compliance AND "service-oriented systems")

Appendix B. Selected primary studies by publisher and publication type.

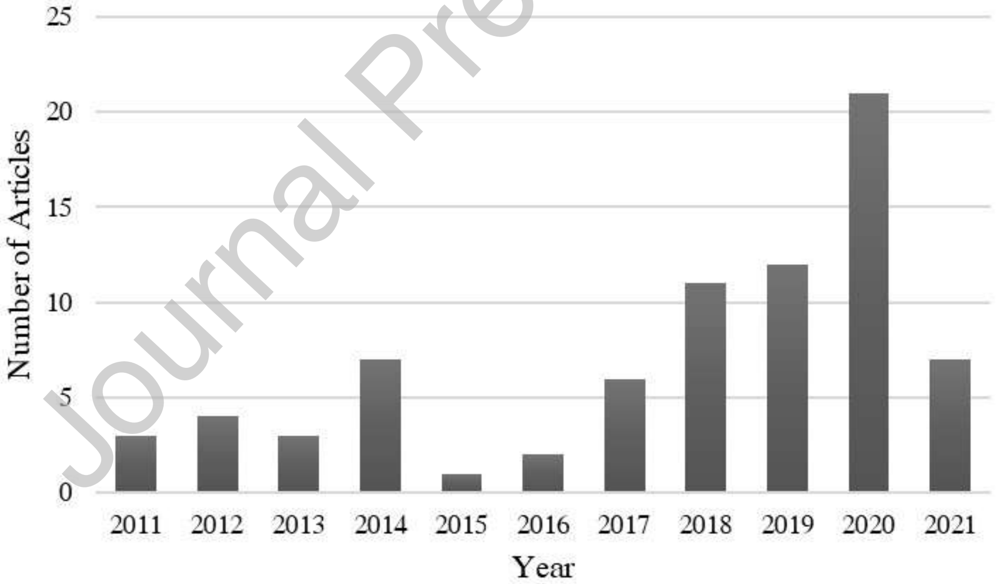
Publisher	Total	Journal	Conference	Workshop
ACM Digital Library	3	-	3	-
Association of Information Systems	4	1	3	-
Atlantis Press	1	1	-	-
Elsevier	18	18	-	-
Emerald	8	8	-	-
Hindawi	1	1	-	-
IEEE Xplore	11	5	4	2
MDPI	4	4	-	-
ProQuest	1	-	1	-
SAGE	3	3	-	-
Springer	8	7	1	-
Taylor & Frances	7	7	-	-
Wiley Online Library	2	2	-	-
World Scientific	1	1	-	-
Other	5	2	2	1
Total	77	60	14	3

Appendix C. Distribution of primary studies based on countries, in which they were conducted in.

Journal Pre-proof

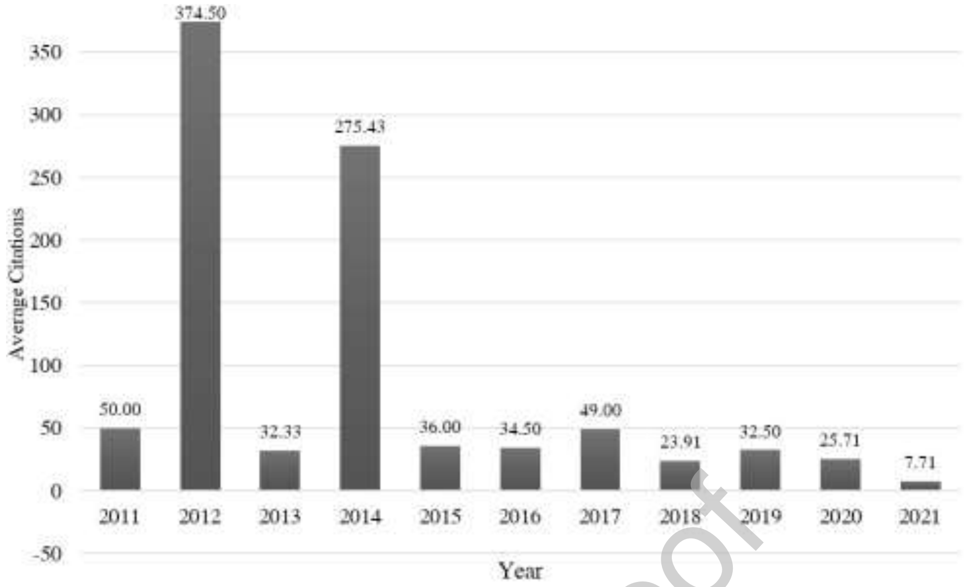


Appendix D. Distribution of the number of primary studies according to the year of publication.



Appendix E. Distribution of average citations of the primary studies per year.

Journal Pre-proof



Appendix F. Theories and their references.

Theory	Reference	Used By
Planned Behavior	[94]	[27], [31], [32], [40], [41], [48], [60], [62], [63], [77], [86], [87], [90]
Deterrence	[105]	[30], [31], [33], [35], [39], [45], [63], [63], [75], [88], [93]
Protection Motivation	[101]	[31], [34], [40], [46], [62], [78], [86], [90], [92]
Rational Choice Theory	[106]	[31], [32], [79], [88]
Social Bond	[107]	[26], [45], [47], [87]
Neutralization	[98]	[38], [90]
Organizational Climate	[108]	[26], [88]
Workarounds	[109]	[82], [91]
Affective Events	[112]	[77]
Reasoned Actions	[113]	[92]
Cognitive Evaluation	[114]	[92]
Cognitive Moral Development	[115]	[31]

Journal Pre-proof

Technostress	[97]	[73]
Moral Disengagement	[116]	[73]
Coping	[117]	[73]
Discourse Analysis	[118]	[28]
Ethical Decision Making	[119]	[38]
Ethical Work Climate	[120]	[63]
Expected Utility	[121]	[63]
Expectancy	[122]	[72]
Information Systems Security	[5]	[71]
Mangle Of Practices	[123]	[80]
Reactance	[124]	[78]
Regulatory Compliance	[125]	[69]
Self-Determination	[126]	[34]
Social Exchange (Guanxi)	[127]	[76]
Technology Threat Avoidance	[128]	[76]
Social Learning	[129]	[93]
Unified Model Of Information Security Policy Compliance	[10]	[74]
Upper Echelon	[130]	[30]
Value Neutrality	[131]	[25]
Value-Based Compliance	[132]	[29]
Work System	[133]	[82]

Journal Pre-proof

Mohammed Mubarkoot is a PhD. Candidate in Technology Management, Economics, and Policy at the College of Engineering at Seoul National University. Prior to that, he worked at

Yemen Telecom as a software developer and systems administrator. His research interest is on software policy compliance and modeling; cloud computing; and open source software policy.

Jörn Altmann is Professor for Technology Management, Economics, and Policy at the College of Engineering at Seoul National University. Prior to this, he has been a postdoc at EECS and ICSI of UC Berkeley, taught computer networks at UC Berkeley, and worked as a senior scientist at Hewlett–Packard Labs. Dr. Altmann's research centres on Internet economics with a focus on economic analysis of Internet services and on integrating economic models into Internet infrastructures.

Morteza Rasti-Barzoki is associate professor at the Department of Industrial and Systems Engineering at the Isfahan University of Technology in Iran. He received his Ph.D. degree from the same university, in 2013. He worked as invited faculty at Industrial Engineering, College of Engineering, Seoul National University for one year (2019-2020). He, also, is a senior researcher at the Technology Management, Economics, and Policy Program at Industrial Engineering, College of Engineering, Seoul National University in 2021. His current research interests include the application of game theory in sustainability, digital supply chain, cybersecurity, and energy.

Bernhard Egger received the diploma in computer science from the Swiss Federal Institute of Technology, Zürich (ETHZ) in 2001 and the PhD degree in computer science and engineering from Seoul National University in 2008. He worked as a senior research engineer at SAIT, Samsung Electronic's research institute, from 2008 to 2011. He joined Seoul National University as a faculty member in 2011 where he currently is a professor in the Department of Computer Science and Engineering. His research interests include programming language design, compilers, and operating systems for heterogeneous manycore systems. He is a member of the IEEE and ACM. More information is available at https://csap.snu.ac.kr/ .

Hyejin Lee is a PhD. Candidate in Technology Management, Economics, and Policy at Seoul National University. Prior to that, she studied engineering and management of technology. Her research interests include technology management in services, changes in socio-economic systems caused by technological development, labor conditions, and skills of workers.

Journal Pre-proof