MARTIN-LUTHER-UNIVERSITÄT
HALLE-WITTENBERG

GEORG-AUGUST-UNIVERSITÄT
GÖTTINGEN IN PUBLICA COMMODA SEIT 1737

Stephan Kühnel • Stefan Sackmann • Simon Trang (Eds.)

CIISR

Current Compliance Issues in Information Systems Research

Proceedings of the First International Workshop on Current Compliance Issues in Information Systems Research (CIISR 2021)

Co-located with the 16th International Conference on Wirtschaftsinformatik (WI 2021)

Online (initially located in Duisburg-Essen, Germany), March 9th, 2021.

16th International Conference on Wirtschaftsinformatik, March 2021, Essen, Germany

Editors

Dr. Stephan Kühnel
Martin Luther University Halle-Wittenberg,
06108 Halle (Saale), Germany

Prof. Dr. Stefan Sackmann
Martin Luther University Halle-Wittenberg,
06108 Halle (Saale), Germany

Prof. Dr. Simon Trang
University of Goettingen,
37073 Göttingen, Germany

Originally published online by CEUR Workshop Proceedings (CEUR-WS.org, ISSN 1613-0073)

Originally published in:

S. Kühnel, S. Sackmann, S. Trang (eds.): Proceedings "Current Compliance Issues in Information Systems Research 2021", CEUR-WS.org/Vol-2966

Preface

to the First International Workshop on Current Compliance Issues in Information Systems Research

Stephan Kühnel[1], Stefan Sackmann[1], Simon Trang[2]

[1] Martin Luther University Halle-Wittenberg, 06108 Halle (Saale), Germany
{stephan.kuehnel, stefan.sackmann}@wiwi.uni-halle.de
[2] Universität Goettingen, 37073 Goettingen, Germany
simon.trang@wiwi.uni-goettingen.de

1 General Description of the CIISR Workshop

"Compliance" refers to rule adherence, i.e., acting in accordance with applicable rules originating from various sources, including laws, standards, contracts, guidelines, etc. [1, 2]. Compliance has been a relevant topic in Information Systems Research (ISR) for several decades, whose initial focus was primarily on the (semi-)automated support in ensuring and validating rule conformity [3–5]. Nowadays, compliance is approached from a variety of different perspectives. As part of information security management, for instance, it is examined which operational compliance measures result in desired employee behavior [6, 7]. In the context of cloud computing, for instance, it is examined how compliance with service level agreements can be ensured in hybrid cloud architectures [8, 9]. And in the context of business process management, for instance, it is examined how the compliance of business processes can be ensured sustainably and economically in digitalized and electronic markets [10–12].

The first *International Workshop on Current Compliance Issues in Information Systems Research (CIISR 2021)* was intended as a prelude to an exchange format that will enable a continuous interchange of scientists and also practitioners in this field. The workshop took place on **March 9th, 2021,** in conjunction with the *16th International Conference on Wirtschaftsinformatik (WI 2021).* Based on the conference's main theme– "Innovation through Information Systems - Business & Information Systems Engineering as a Future-Oriented Discipline"–the CIISR workshop discussed current compliance issues with high relevance to the ISR area.

16th International Conference on Wirtschaftsinformatik,
March 2021, Essen, Germany

2 Submission and Paper Selection

We invited the scientific community to submit discussion papers and also research results as contributions to the CIISR 2021 workshop. Submissions in numerous subject areas interfacing with compliance were welcome, such as ensuring compliance with information security policies, compliance issues in the context of clouds, ensuring business process compliance, current IT compliance issues, and–for a given current occasion–the impact of the COVID-19 pandemic on compliance in the ISR environment. We called for contributions from the above-mentioned topics that can be assigned to one of the following three submission types:

1. **Completed research papers/completed practical reports**
   This submission type includes both advanced research with at least partial evaluation and comprehensive practical contributions.
2. **Short papers (research in progress papers/short practical reports)**
   Short papers represent ongoing research or ongoing practical projects. In addition to presenting initial results, these papers should also include an outlook on further research or project progress, including planned future work steps.
3. **Extended abstracts**
   Extended abstracts present and discuss high-quality results of already published contributions (or dissertations/postdoctoral theses) relevant to the workshop topic.

In the submission version, completed research papers and practical reports must not exceed 12 pages, short papers must not exceed six pages, and extended abstracts must not exceed four pages, including title, abstract, bibliography, author details, and acknowledgments. Possible appendices are not included in the pagination.
Each paper submitted to the workshop underwent a rigorous double-blind review by at least two reviewers and was evaluated for five criteria: 1) quality of content, 2) significance for theory and practice, 3) originality and level of innovativeness, 4) fitting to the workshop theme, and 5) quality of presentation. The three workshop chairs subsequently discussed the review results of each paper, resulting in a decision of acceptance or rejection. A total of seven papers were submitted to the workshop, of which four were accepted as full papers and one as a short paper. Accordingly, the acceptance rate of full papers was 57 %.

3 CIISR 2021 Workshop Papers

In line with the WI 2021, the CIISR 2021 workshop was held completely online. Despite its virtual form, we are pleased to report that it was well received by the research community. 42 conference attendees were registered for the workshop, and finally, more than 50 attended. The CIISR 2021 workshop and the CIISR 2021 workshop proceedings at hand contain six contributions, including one paper on the keynote speech of the workshop chairs, the four accepted full papers, and one accepted short paper:

1. The paper **Towards a Business Process-based Economic Evaluation and Selection of IT Security Measures** accompanies the keynote and particularly focuses on the ProBITS project, which is funded by the German Federal Ministry of Education and Research (BMBF) since April 2021 and deals with the economic assessment and analysis of IT security measures in business processes.
2. The full paper **Analysis of Public Cloud Service Level Agreements–An Evaluation of Leading Software as a Service Providers** by Michael Seifert analyses compliance in the context of cloud computing. His research is devoted to comparing service level agreements and reducing their heterogeneity. In this context, the paper also sheds light on the management of compliance with agreed-upon requirements.
3. The full paper **Software Compliance in Different Industries: A Systematic Literature Review** by Mohammed Mubarkoot and Joern Altmann analyses compliance of software and software services. Based on a systematic literature review, existing frameworks of software compliance management are identified and compared to the needs of different industries. The results show heterogeneity in terms of approaches and industries, especially regarding priorities, specifics, and compliance requirements, so further research seems to be vital.
4. The full paper **Reviewing the Interrelation Between Information Security and Culture: Toward an Agenda for Future Research** by Sebastian Hengstler and Natalya Pryazhnykova is dedicated to analyzing the relevance of culture to information security on different levels. Their results show that cultural aspects are relevant in different areas of information security, namely in information security governance, in awareness programs, in its influence on compliance behavior, and when designing an organizational security culture. They propose to further analyze the connection between culture and information security in the light of their identified research areas to better understand the impact of culture on security compliance.

5. The full paper **Culture Matters–A Cross-Cultural Examination of Information Security Behavior Theories** by Sebastian Hengstler empirically compares different theories for ensuring information security compliance behavior with respect to different cultures. Protection motivation and deterrence theory are tested in Germany, India, and the USA and compared by invariance tests and determination of predictive power. The conclusion suggests that taking a differentiated view on culture might improve information security policy compliance behavior in the future.
6. The short paper **MIA–A Method for Achieving Compliance in Flexible and IT Supported Business Processes** by Tobias Seyffarth presents a holistic framework for managing business process compliance in flexible environments. His research models relations between compliance requirements, business process activities, and underlying IT components. Thus, the approach allows interesting analyses of these relations, especially when changes become necessary.

4 Organization and Acknowledgement

The main person responsible for the workshop was Dr. Stephan Kühnel (general workshop and web chair), who was supported by Prof. Dr. Stefan Sackmann and Prof. Dr. Simon Trang (workshop co-chairs). Stephan Kühnel and Stefan Sackmann are researchers in the field of business process management at the Chair for Information Systems, esp. Business Information Management at the Martin Luther University Halle-Wittenberg. Both are actively researching in the field of economic evaluation of business process compliance and security. Simon Trang is a researcher in the field of information security management and holds the Chair for Information Security and Compliance at the Georg August University of Goettingen. His research focuses on the economic aspects of information security measures and human aspects of information security.
Although the number of submissions to the workshop was manageable, establishing a new workshop in the community would not have been possible without the help of others. Thus, we are very thankful for all the support we received from the teams of the respective chairs. Furthermore, we are very thankful for all the support we got during the review process. We were happy to have so many researchers supporting us in the program committee, namely (in alphabetic order of the last name):

- Michael Fellmann (University of Rostock, Germany),
- Barbara Gallina (Maelardalen University, Sweden),
- Nadine Guhr (Leibniz University Hannover, Germany),
- Simon Hacks (KTH Royal Institute of Technology Stockholm, Sweden),

- Martin Schultz (HAW University of Applied Sciences Hamburg, Germany),
- Michael Seifert (GISA GmbH, Germany),
- Tobias Seyffarth (Martin Luther University Halle-Wittenberg, Germany),
- Frank Teuteberg (Osnabrueck University, Germany), and
- Nils Urbach (University of Bayreuth, Germany).

In addition, we thank Peter Hofmann (University of Bayreuth, Germany) and Sebastian Hengstler (Georg August University of Goettingen, Germany) for their work as (sub)reviewers. Last but not least, our thanks also belong to Sebastian Lindner (Martin Luther University Halle-Wittenberg, Germany) for his work as a web co-chair and to the WI 2021 team for their support in organizational and technical matters.

References

1. Becker, J., Delfmann, P., Dietrich, H.-A., Steinhorst, M., Eggert, M.: Business Process Compliance Checking – Applying and Evaluating a generic Pattern Matching Approach for Conceptual Models in the Financial Sector. Information Systems Frontiers 18, pp. 359–405, (2016).
2. Rinderle-Ma, S., Ly, L.T., Dadam, P.: Business Process Compliance (Aktuelles Schlagwort). EMISA Forum, pp. 24–29, (2008).
3. Sackmann, S., Kuehnel, S., Seyffarth, T.: Using Business Process Compliance Approaches for Compliance Management with Regard to Digitization: Evidence from a Systematic Literature Review. In: Weske M., Montali M., Weber I., vom Brocke J. (eds) Business Process Management. BPM 2018. Lecture Notes in Computer Science, vol 11080. Springer, Cham, pp 409-425, (2018).
4. Fellmann, M., Zasada, A.: State-of-the-art of Business Process Compliance Approaches: A Survey. Proceedings of the 22nd European Conference on Information Systems (ECIS'14), pp. 1–17, (2014)
5. Schultz, M.: Towards an Empirically Grounded Conceptual Model for Business Process Compliance. In: Ng W., Storey V.C., Trujillo J.C. (eds) Conceptual Modeling. ER 2013. Lecture Notes in Computer Science, vol 8217. Springer, Berlin, Heidelberg, pp 138-145, (2013).
6. Trang, S., Brendel, B.: A Meta-Analysis of Deterrence Theory in Information Security Policy Compliance Research. Information Systems Frontiers 21, pp. 1265–1284, (2019)
7. Lembcke, T.-B., Masuch, K., Trang, S., Hengstler, S., Plics, P., Pamuk, M.: Fostering Information Security Compliance: Comparing the Predictive Power of Social Learning Theory and Deterrence Theory. Americas Conference on Information Systems (AMCIS), (2019).
8. Xiaoyong, Y., Ying, L., Tong, J., Tiancheng, L., Zhonghai, W.: An Analysis on Availability Commitment and Penalty in Cloud SLA. In: Computer Software and Applications Conference (COMPSAC), pp. 914–919, (2015).

9. Morin, J.-H., Aubert, J., Gateau, B.: Towards Cloud Computing SLA Risk Management: Issues and Challenges. In: Sprague, R.H. (ed.) 45th Hawaii International Conference on System Sciences. (HICSS) ; USA, 4 - 7 Jan. 2012, pp. 5509–5514, (2012).
10. Seyffarth, T., Kuehnel, S., Sackmann, S.: Business Process Compliance Despite Change: Towards Proposals for a Business Process Adaptation. In: Cappiello C., Ruiz M. (eds) Information Systems Engineering in Responsible Information Systems. CAiSE 2019. Lecture Notes in Business Information Processing, vol 350. Springer, Cham, pp. 227-239, (2019).
11. Kuehnel, S., Trang, S., Lindner, S.: Conceptualization, Design, and Implementation of EconBPC – A Software Artifact for the Economic Analysis of Business Process Compliance. In: Laender A., Pernici B., Lim EP., de Oliveira J. (eds) Conceptual Modeling. ER 2019. Lecture Notes in Computer Science, vol 11788. Springer, Cham, pp. 378-386, (2019).
12. Knuplesch, D., Reichert, M., Fdhila, W., Rinderle-Ma, S.: On Enabling Compliance of Cross-Organizational Business Processes, In: Daniel F., Wang J., Weber B. (eds) Business Process Management. Lecture Notes in Computer Science, vol 8094. Springer, Berlin, Heidelberg, pp. 146-154, (2013).

Towards a Business Process-Based Economic Evaluation and Selection of IT Security Measures

Keynote

Stephan Kühnel[1], Stefan Sackmann[1], Simon Trang[2], Ilja Nastjuk[2], Tizian Matschak[2], Laura Niedzela[1], Leonard Nake[1]

[1] Martin Luther University Halle-Wittenberg, 06108 Halle (Saale), Germany
{stephan.kuehnel, stefan.sackmann, laura-maria.niedzela, leonard.nake}@wiwi.uni-halle.de
[2] Universität Goettingen, 37073 Goettingen, Germany
{simon.trang, ilja.nastjuk, tizian.matschak}@wiwi.uni-goettingen.de

1 Introduction

Technological innovations, such as cloud computing, intelligent process automation, and big data analytics offer substantial opportunities for maintaining and strengthening a company's competitive position. However, the introduction of such technologies entails new compliance and security risks. One of the most challenging risks that companies face is to protect technologies and other organizational assets from incidents or attacks that aim to access sensitive information (confidentiality attacks), change the code or data in information systems (integrity attacks), as well as disrupt the normal operation of information systems (availability attacks) [1].

To mitigate such risks, both legislators and companies define far-reaching and overarching requirements for information, data, and information technology (IT) security. Examples can be found in a company's information security governance requirements (e.g., general policies on authentication or guidelines on data classification and handling), in sector-specific guidelines (e.g., the second Payment Services Directive of the European Union (EU) for banks), or in cross-sectoral regulations (e.g., the EU General Data Protection Regulation (GDPR) or the German IT Security Act). It is essential for companies to comply with such requirements, i.e., to implement the requirements through adequate IT security measures.

16th International Conference on Wirtschaftsinformatik,
March 2021, Essen, Germany

IT security measures are mechanisms that support organizations to identify and alert about security incidents, to protect critical infrastructure services with the aim to preserve the confidentiality, integrity, and availability of information, to respond to security incidents (e.g., reduce the number of successful attacks), and to recover system integrity after a security incident [2]. IT security measures include both technical measures, such as firewalls, intrusion detection systems, or authentication mechanisms, as well as human-centric measures, such as information classification policies, clean-desk regulations, and password policies [3]. In most cases, the implementation of extensive IT security requirements cannot be realized through isolated IT security measures but requires a complex bundle of interdependent measures. On the one hand, such measures entail high investment costs and, on the other hand, can significantly influence companies' business processes. For example, Article 32 (1) of the GDPR requires that appropriate technical and organizational measures should be implemented to ensure compliance with the protection goals of confidentiality, integrity, availability, and resilience when processing personal data. To implement this requirement, both technical precautions (e.g., encryption and pseudonymization of personal data) and procedural configurations (e.g., activities and controls to ensure compliance in business processes) are necessary. Such technical precautions and procedural configurations can lead to high expenses [4, 5]. It is therefore not surprising that compliance with IT security requirements is already described in existing literature as a cost-intensive task [6, 7] and even as a "heavy cost driver" [8].

Consequently, "*the focus of IT security management is shifting from what is technically possible to what is economically efficient*" ([9], p. 66). To ensure that a company's profitability is not affected by implementing bundles of IT security measures, it becomes necessary to identify suitable alternative courses of action to meet IT security requirements and select the best alternatives based on economic criteria [10]. Accordingly, the evaluation and selection of IT security measures have become critical skills for information security managers. Traditional investment-based approaches and theories, such as the return on investment (ROI), the real options theory (ROT), or the utility maximization theory (UMT), form the backbone of most contemporary methods to economically evaluate IT security investment decisions [11]. In the context of IT security, widely accepted methods to evaluate the return on investment include the return on security investment (ROSI) and the return on information security investment (ROISI) [12]. Such methods consider directly attributable monetary costs and benefits, which become important determinants of investment decisions. Decision makers benefit from utilizing investment-based evaluation methods because they enforce to think about explicit assumptions and decision rationales. In addition, they help to understand whether security investments are consistent with the organizational risk strategies [13].

However, investment-based approaches offer only limited guidance for the decision to implement IT security measures because of the lack of available data to generate accurate results, the high dependency of these approaches on subjective assumptions, and the negligence to account for the interdependency between multiple IT security

measures [11]. In addition, investment-based methods usually do not account for non-monetary and indirect effects, such as the impact of IT security measures on business process performance or outcome. This is an important topic of interest for two reasons. First, IT investments in general impact the efficiency of business processes [14], and second, business processes have a substantial impact on the competitive position and financial performance of any organization [15].
Since business processes are at the center of a company's success, they offer a solid foundation for cost-benefit analysis [16]. However, to the best of our knowledge, there is a lack of approaches in the literature supporting a comprehensive economic evaluation of IT security measures (and bundles of measures) with particular regard to their interaction with business processes. Based on existing knowledge about contemporary business process management and compliance, we propose several requirements for the development of business process-driven approaches to the evaluation and selection of IT security measures for guiding future research. In particular, the paper discusses the requirements needed on the journey towards a process-based approach for the economic evaluation and selection of IT security measures. Such an approach enables effective selection and implementation of IT security measures, stimulates business process improvement, and further offers the opportunity to overcome the limitations of existing investment-based methods.

2 Important Investment-based Approaches for the Economic Evaluation of IT Security Measures

As mentioned above, investment theories form the backbone of most existing methods for the economic evaluation of IT security measures [11]. In this context, direct costs for the introduction and operation of (mostly isolated) IT security measures (e.g., costs for software, hardware, or personnel) are interpreted as an investment from which an expected direct return on capital (monetary benefit) results [17]. The existing literature on the evaluation of IT security measures is dominated by the following three approaches [11]:

1. Approaches based on the ROI (see, e.g., [18]), which value the return on investment generated by an isolated IT security measure relative to the capital invested.
2. Approaches based on the ROT (see, e.g., [19]), which are based on option pricing models for the valuation of IT security investments taking into account time-dependent variability.
3. Approaches based on the UMT (see, e.g., [20]), which aim to maximize the benefit of an IT security investment for a given subject.

All three approaches share the assumption that the capital reflow is represented by the expected proportion of monetary damage from a potential IT security incident that can

be prevented by the use of an IT security measure, such as prevented operational downtime or avoided recovery costs of an attack [21]. Based on these approaches, different methods have been discussed in the literature to economically evaluate IT security measures (for a detailed survey, see [11]). In the following, we would like to present an important selection of these.

2.1 The Annual Loss Exposure

In 1979, the National Bureau of Standards of the U.S. Department of Commerce introduced the Annual Loss Exposure (ALE) as a first method to assess IT security risks. ALE can be used to estimate the monetary annual loss exposure of a company based on the damage that results from security incidents (impact) and the likelihood of such an incident occurring (frequency of occurring) [22]. For single security incidents, the ALE is simply computed by multiplying the estimated impact (e.g., expressed as a monetary value) by the expected occurrence frequency. If there are several security incidents, the ALE totals the product of the two variables for each security incident (summation) [23]. As a single metric, ALE is not sufficient to accurately perform an economic evaluation of IT security measures, but usually represents an input variable for more complex evaluation procedures (see, e.g., [5, 23–25]).

2.2 Return on Security Investment

The ROSI is based on the traditional ROI calculation and compares the benefits of IT security measures with their costs [21, 26, 27]. It considers the probability of occurrence of an IT security incident, loss prevention due to an IT security measure, the cost of security incidents, and the costs of IT security measures. While the costs of an IT security measure correspond to the investment costs, benefits are determined by reducing the probability of occurrence of security incidents and reducing the amount of loss due to the implementation of the IT security measure. Sonnenreich et al. [5] suggest that the ALE can be used to calculate ROSI. Thereby the ALE is multiplied by an effectiveness parameter, which provides information on the effectiveness of IT security measures (expressed as a percentage). The result represents the portion of the monetary annual expected loss value that can be saved by implementing IT security measures. Then, the total costs resulting from the implementation of IT security measures are subtracted to determine the net financial "return." Finally, the net financial return is divided by the total costs to produce a relative ROSI value. Per classical ROI interpretation, an investment in IT security measures is economically advantageous if it holds that $ROSI > 0$. If the $ROSI < 0$, IT security investments are financially not viable and, thus, should be avoided for economic reasons. For $ROSI=0$, the monetary advantages and disadvantages are balanced. Further alternatives to calculate the ROSI are based on a direct

comparison of costs incurred due to a security incident and total costs for implementing and operating IT security measures (see, e.g., [28–30]).

2.3 Return on Information Security Investment

Another model for evaluating IT security measures is Mizzi's Return on Information Security Investment (ROISI) [31]. In alignment with ROSI, ROISI considers the security expenditures based on one-time costs to implement a defense mechanism, maintenance costs, and costs to fix system vulnerabilities. The potential total loss resulting from security incidents is conceptualized based on missed revenue and information lost due to system downtimes and the financial costs of rebuilding the system (e.g., labor costs for system recovery). The main difference to the ROSI method is that Mizzi's approach includes a cost-benefit consideration of the malicious entity. To determine ROISI, Mizzi defines the cost of an attack as the cost of penetrating the security mechanism and exploiting vulnerabilities. A rational attacker only carries out an attack (in the sense of ROSI this means influencing the probability of occurrence) if the benefit accruing to the attacker is greater than his costs. The rationale behind this assumption is that a rational attacker is usually unwilling to pay more for an attack than the immediate loss suffered by the attacked entity (e.g., the value of the stolen information). Mizzi suggests that IT security measures should be designed to maximize attackers' costs and minimize the information potentially accessible.

2.4 Adapted Loss Database

Sackmann and Syring [32] base the evaluation of IT security measures or security adaptations of technical infrastructures on the protection goals of business processes. In this context, changes are modeled in a binary way from the perspective of an IT risk reference model and based on a cause-and-effect concept that maps the chain from threats to attacks and vulnerabilities to business processes. For the evaluation of both isolated security measures and bundles of measures, the original data (e.g., historical damages) are adapted to a more realistic cause-and-effect model and, thus, recalculated. In principle, the adaptation of the data basis could be used with any method (e.g., ROSI) for an evaluation of the measures under consideration.

2.5 Cyber Investment Analysis Methodology

The Cyber Investment Analysis Methodology (CIAM) is a four-step data-driven approach to evaluate and select IT security measures [33]. First of all, it is necessary to collect and/or select data on the assets to be protected, including data on security incidents, appropriate IT security measures, the impact of exploited vulnerabilities on the

business, and costs to implement IT security measures. The second step involves estimating weightings by domain experts to understand how each IT security measure contributes to the goals of prevention, detection, and recovery. The third step includes performing an effectiveness scoring in which each IT security measure is matched against each attack step. Finally, an algorithm uses the data to compute a relative priority ranking for each IT security measure.

2.6 Security Attribute Evaluation Method

Butler [13] proposes the Security Attribute Evaluation Method (SEAM) as an economic approach for assessing security investments. SAEM also proposes four steps to perform the cost-benefit analysis of security measures. First, it starts with an assessment of the benefits of an IT security measure. The second step includes evaluating the effectiveness of the IT security measure in mitigating security risks. Third, a threat coverage assessment is performed. The final step involves an assessment of the costs of the IT security measure. Butler suggests that the data needed for the evaluation is sourced from structured interviews with IT and security experts. To successfully conduct a SEAM analysis, the company must have effective IT security policies and procedures in place, have security mechanisms properly integrated into the existing IT infrastructure, and be able to accurately predict attacks and their associated consequences.

3 Limitations of Existing Evaluation Methods for IT Security Measures

While the methods presented in the previous chapter are valuable to evaluate and select appropriate IT security measures economically, they offer several limitations.
One limitation is related to the **lack of multidimensionality**. Besides having an impact on monetary returns, IT security measures have non-monetary effects. For example, they can impact employee behavior, the organization's reputation, as well as process complexity or flexibility [4, 5]. Investment theory-based evaluation methods usually do not account for such effects [11]. Accordingly, the scope and coverage of existing approaches need to be extended to also include the impact of IT security measures on non-financial dimensions.
Another limitation is related to the **lack of valid data** for calculation. It is one of the biggest challenges for organizations to obtain accurate data on the true costs of a security incident. Most methods are data-driven, although necessary input data or accurate estimators are often unavailable [11, 17]. Decision makers frequently underestimate the costs of security incidents by looking only at the short-term tangible costs (e.g., lost revenue), but there are also long-term intangible costs (e.g., loss of trust) that are difficult to measure and therefore often neglected [9]. Another reason for the lack of valid data is that most companies do not proactively and accurately capture cost information,

as emphasized by Sonnenreich et al. ([5], p.47): "*Security breaches that have no immediate impact on day-to-day business often go completely unnoticed. When a breach does get noticed, the organization is usually too busy fixing the problem to worry about how much the incident actually costs. After the disaster, internal embarrassment and/or concerns about public image often result in the whole incident getting swept under the rug. As a result of this "ostrich response" to security incidents, the volume of data behind existing actuarial tables is woefully inadequate*."

Another limitation is related to the **lack of comparability**. It is often difficult to compare IT security measures, which are characterized by different goals and scopes based on a monetary **assessment** of costs and benefits alone. In this context, Butler [13] emphasizes that it is more difficult to compare benefits among different IT security measures than comparing costs. Existing and proven financial analysis tools allow costs to be estimated quite accurately, but benefits are more difficult to quantify since they are usually characterized by greater uncertainty, time lag, and indirect effects. In addition, decision-makers are often confronted with imperfect knowledge about the explicit benefits of IT security measures. Therefore, estimating costs and benefits often depends on the IT security experts' intuition, practical expertise, knowledge, and experience.

Research has also criticized the **lack of scalability** of existing evaluation methods (see, e.g., [9, 11]). Investment-based methods are sensitive to different business sizes. Although large corporations as well as small and medium-sized enterprises (SMEs) are equally affected by IT security requirements, SMEs often have fewer financial and personnel resources. For instance, Sonnenreich et al. [5] emphasize that the cost-benefit ratio of security investments is increasingly skewed as the number of employees decreases, which is the case for most SMEs compared to large corporations. They exemplify how an initially financially viable investment in an anti-spam solution would not have been viable if the same organization were smaller, i.e. had fewer employees.

Finally, the presented methods are usually aimed at the **evaluation of isolated IT security measures**, but they do not account for the effects that IT security measures have on other measures when implemented as a bundle. Understanding synergies between IT security measures is important to achieve desired business outcomes [34]. In this context, Axelsson ([35], p. 189) emphasizes: "*The best effect is often achieved when several security measures are brought to bear together. How should intrusion detection collaborate with other security mechanisms to achieve this synergy effect? How do we ensure that the combination of security measures provides at least the same level of security as each applied singly would provide, or that the combination does not in fact lower the overall security of the protected system?*" No single IT security measure can ensure security by itself, and therefore, they need to be implemented in bundles and configured to achieve optimal outcomes [36]. In this regard, Cavusoglu et al. [9] criticize investment-based approaches as they do not consider the potential positive and negative interactions of different IT security measures. More concretely, they criticize

the assumption that implementing one security measure will reduce the number of attacks by a certain percentage and will result in a certain benefit value, as this neglects substitution and complementary effects with other existing IT security measures.
The next chapter discusses how business process management concepts can contribute to overcoming some of the limitations outlined.

4 A Journey Towards a Process-Based Approach to Selecting and Evaluating IT Security Measures

Using contemporary business process management concepts offers a promising approach to address some of the key limitations outlined in the previous chapter. At the core of business process management are business processes, which are defined as a structured sequence of activities designed to achieve a specific output [37].

4.1 Two Interesting Approaches as Examples of How Business Process Management Can Already Be Used to Evaluate

Magnani and Montesi [38, 39] proposed an approach for the cost evaluation of business processes. The authors suggest extending relevant process elements in a business process model with cost annotations. Costs are represented as textual information at the respective process elements. Such an approach reaches its limits if business processes are nested, i.e., if they contain one or more subprocesses and the calculation of costs depends on their sequence flows. This is the case, for example, if a subprocess contains connectors of the XOR type. The authors propose two alternatives for this limitation. The first involves annotating cost intervals instead of individual cost values to all flow objects (including subprocesses). Processes with fully annotated cost intervals are suitable for the application of graph-based algorithms to determine the minimum and maximum costs. For example, Dijkstra's algorithm [40] can be applied to identify a minimum cost path between start and end events in a business process. However, it is challenging to use cost intervals when loops are included in subprocesses since the upper interval tends towards infinity in this case. The second alternative addresses this problem by calculating and annotating average costs, provided that data from a sufficiently large sample of process instances are available. However, the accuracy of the calculation of average costs depends on the availability and correctness of data. The authors demonstrate the applicability of both alternatives using the example of hotel reservations.
Sampathkumaran and Wirsing [41, 42] present a similar approach focused on determining the expected costs of successfully executing a process, which they refer to as "business costs." In contrast to Magnani and Montesi [38, 39], this approach does not only focus on the determination of costs but also the degree of achievement of a defined

business objective. To include this degree in the calculation, the authors extended the approach of Magnani and Montesi with the concept of "reliability" in calculating process costs. Reliability represents the probability of successful execution of a task that an organization performs to achieve a specific (business) objective. Consequently, the business costs of a process depend not only on the costs of the process itself (e.g., the amount of money needed to execute a process) but also on the process reliability (e.g., factors leading to successful process completion and the achievement of business objectives). Sampathkumaran and Wirsing additionally suggest performing sensitivity analyses to identify parameters that have the most critical impact on the business costs and to optimize the process model.

4.2 Requirements for a Process-Based Approach to the Economic Evaluation and Selection of IT Security Measures

The aforementioned approaches can also be applied to IT security measures implemented in business processes if specific conditions are met (e.g., modeling IT security measures as modular and thus interchangeable subprocesses). Thus, they can provide valuable information for determining the additional costs of IT security measures. However, they do not accurately capture the interdependence between IT security and business performance, i.e., how IT security measures impact the performance of business processes. This is important to understand in order to improve the decision-making process for IT security measures. We argue that a process-based approach for the economic evaluation and selection of IT security measures offers tremendous opportunities to complement existing approaches and overcome their limitations. Still, for the successful implementation of a process-based evaluation approach in the context of IT security, several requirements have to be taken into account.

The development of a process-based approach requires, as a first step, the identification of factors that characterize a business process and allow for its performance determination. For example, complexity is a common characteristic of a business process that significantly impacts associated quality and cost [43, 44]. The implementation of IT security measures can lead to either a reduction or an increase in the complexity of a business process and thus influence the cost-effectiveness of achieving business goals. For example, Stoewer and Kraft [45] show that new security solutions can lead to improved process efficiency if the IT security measure to be implemented triggers a redesign of the underlying process. Therefore, we argue that a prerequisite for a process-based approach to assessing IT security measures is to capture relevant factors that characterize business processes and impact their performance. However, it is important to consider that business processes have different and possibly competing priorities in terms of factors such as time, cost, flexibility, or quality [46]. In this regard, vom Brocke and Sonnenberg [47] emphasize the importance of considering trade-offs be-

tween factors when determining the economic value of business processes: "*[…] a process that produces quality products might have long cycle times and relatively high costs, whereas a process with low cycle times might have moderate costs and a low quality level*" (p. 114). A goal-oriented approach is desirable to appropriately manage competing priorities in business processes. Goal orientation accounts for the strategic objectives of an organization and how these objectives are achieved through business process design [48]. Consequently, a process-driven approach requires a definition and evaluation of the specific business process goals.

Once relevant influencing factors are identified, the next step is to investigate which business processes are affected by IT security measures. Standards such as the Business Process Modeling and Notation (BPMN) allow for the graphical modeling and specification of business process models [49]. Business process models provide specific insights into how organizations work and we argue that they offer the opportunity to integrate IT security measures into their process landscape, as shown by Seyffarth et al. [50]. One example is the implementation of so-called access controls to monitor and control access to organizational systems for ensuring the integrity and confidentiality of data [51]. Access controls can be mapped in business process models by specific modeling objects such as tasks, events, gateways, and annotations. In a purchase-to-pay scenario, Sadiq et al. [52] demonstrate that compliance controls can be integrated into an organizational process model through specific process annotations (so-called control tags).

The next step involves quantitatively evaluating the extent to which a process model is influenced by the integration of IT security measures. Kuehnel et al. [53] use so-called process log files as the data basis for their calculations in the context of compliance measures. They propose various design requirements and principles for an IT tool that is supposed to enable an economic evaluation of business process compliance. For example, the IT tool should be able to automatically reconstruct the paths of a business process from a given log file and support a modular process view to visualize compliance activities. We argue that log files can be used to capture the performance of a business process and any changes caused by the implementation of IT security measures. It should be noted that the economic analysis of IT security measures based on business processes is a "complex task" that can overwhelm the person in charge (e.g., the process owner or IT security expert), especially if log files are analyzed manually [53]. Considering that the main goal of human decision-makers is to optimize decision quality with the least possible cognitive effort, the use of software artifacts is recommended (e.g., [53–55]).

The development and evaluation of a process-based approach for the economic evaluation of IT security measures should also be performed in close cooperation with businesses of different sizes and types. This is important since large corporations differ from small and medium-sized corporations, for example, in terms of available resources, processes, security requirements, and security expertise [56, 57]. In addition, IT security requirements and associated business processes vary across industries. For

example, information systems from electricity suppliers that rely on smart meters to exchange information with other devices in a smart grid have specific infrastructure requirements and different system vulnerabilities than information systems from the healthcare sector [58, 59]. Understanding and accounting for such differences when developing a process-based approach to the economic evaluation of IT security measures contributes to the early identification of gaps and missing requirements and supports broad applicability.

5 Conclusion

Selecting the best set of IT security measures is an important strategic decision for any organization, considering the costs associated with security incidents and the significant impacts on the organization's business processes. Therefore, the ability to accurately evaluate the costs and benefits associated with IT security investments has become a critical skill for decision-makers. Traditional (investment-based) approaches provide only limited guidance in determining the true costs and benefits of IT security measures. We, therefore, discuss the journey towards a process-based approach to economically evaluating and selecting IT security measures. We argue that it is important to account for the interdependencies between IT security measures and business processes, as business processes form the backbone of an organization's business model and are key cost and performance drivers. Although a process-based approach cannot address all shortcomings of traditional methods, it has the potential to improve the quality of strategic IT security investment decisions.

References

1. Gunduz, M.Z., Das, R.: Cyber-security on smart grid: Threats and potential solutions. Computer Networks 169, 107094 (2020)
2. Information Systems Audit and Control Association (ISACA): Implementing the NIST Cybersecurity Framework. ISACA, Rolling Meadows, IL (2014)
3. Trang, S., Brendel, B.: A Meta-Analysis of Deterrence Theory in Information Security Policy Compliance Research. Information Systems Frontiers 21, 1265–1284 (2019)
4. Kühnel, S., Sackmann, S., Seyffarth, T.: Effizienzorientiertes Risikomanagement für Business Process Compliance. HMD 54, 124–145 (2017)
5. Sonnenreich, W., Albanese, J., Stout, B.: Return On Security Investment (ROSI): A Practical Quantitative Model. Journal of Research and Practice in Information Technology 38, 45–56 (2006)
6. Sadiq, S., Governatori, G.: Managing Regulatory Compliance in Business Processes. In: Vom Brocke, J., Rosemann, M. (eds.) Handbook on Business Process Management 2. Strategic Alignment, Governance, People and Culture, pp. 265–288. Springer Berlin Heidelberg, Berlin, Heidelberg, s.l. (2015)

7. La Rosa, M.: Strategic business process management. International Conference on Software and Systems Process (ICSSP) (2015)
8. Becker, J., Delfmann, P., Dietrich, H.-A., Steinhorst, M., Eggert, M.: Business process compliance checking – applying and evaluating a generic pattern matching approach for conceptual models in the financial sector. Information Systems Frontiers 18, 359–405 (2016)
9. Cavusoglu, H., Cavusoglu, H., Raghunathan, S.: Economics of IT Security Management: Four Improvements to Current Security Practices. CAIS 14 (2004)
10. Sackmann, S.: A Reference Model for Process-oriented IT Risk Management. ECIS 2008 Proceedings (2008)
11. Schatz, D., Bashroush, R.: Economic valuation for information security investment: a systematic literature review. Information Systems Frontiers 19, 1205–1228 (2017)
12. Tsiakis, T., Stephanides, G.: The economic approach of information security. Computers & Security 24, 105–108 (2005)
13. Butler, S.A.: Security attribute evaluation method: a cost-benefit approach. Proceedings of the 24th International Conference on Software Engineering (ICSE 2002), 232–240 (2005)
14. Tallon, P.P.: A Process-Oriented Perspective on the Alignment of Information Technology and Business Strategy. Journal of Management Information Systems 24, 227–268 (2007)
15. Ray, G., Barney, J.B., Muhanna, W.A.: Capabilities, business processes, and competitive advantage: choosing the dependent variable in empirical tests of the resource-based view. Strat. Mgmt. J. 25, 23–37 (2004)
16. Kuehnel, S., Zasada, A.: An Approach Toward the Economic Assessment of Business Process Compliance. In: Woo, C., Lu, J., Li, Z., Ling, T.W., Li, G., Lee, M.L. (eds.) Advances in Conceptual Modeling. ER 2018 Workshops Emp-ER, MoBiD, MREBA, QMMQ, SCME, Xi'an, China, October 22-25, 2018, Proceedings, pp. 228–238. Springer International Publishing, Cham (2018)
17. Davis, A.: Return on security investment – proving it's worth it. Network Security 2005, 8–10 (2005)
18. Pulliam Phillips, P., Phillips, J.J.: ROI fundamentals. Why and when to measure ROI. Pfeiffer, San Francisco (2008)
19. MILLER, L.T., PARK, C.S.: Decision Making Under Uncertainty—Real Options to the Rescue? The Engineering Economist 47, 105–150 (2002)
20. Strotz, R.H.: Myopia and Inconsistency in Dynamic Utility Maximization. The Review of Economic Studies 23, 165 (1955)
21. Soo Hoo, K.J.: How Much is Enough? A Risk Management Approach to Computer Security. Working Paper. Stanford University (2000)
22. National Bureau of Standards: Guideline for Automatic Data Processing Risk Analysis. Federal Information Processing Standards Publication (FIPS PUB) Nr. 65
23. Sackmann, S., Hofmann, M., Kühnel, S.: Return on Controls Invest. HMD 50, 31–40 (2013)

24. Kühnel, S., Sackmann, S.: Effizienz Compliance-konformer Kontrollprozesse in internen Kontrollsystemen (IKS). HMD 51, 252–266 (2014)
25. Rumpel, R., Glanze, R.: Verfahren zur Wirtschaftlichkeitsanalyse von IT-Sicherheitsinvestitionen. Practical Business Research 2, 1–12 (2008)
26. Fox, D.: Betriebswirtschaftliche Bewertung von Security Investments in der Praxis. Datenschutz und Datensicherheit (DuD) 35, 50–55 (2011)
27. Wei, H., Frinke, D., Carter, O., Ritter, C.: Cost-Benefit Analysis for Network Intrusion Detection Systems. Proceedings of the CSI 28th Annual Computer Security Conference (2001)
28. Dirk Schadt: Über die Ökonomie der IT-Sicherheit - Betrachtungen zum Thema "Return on Security Investment. HMD Prax. Wirtsch. 248 (2006)
29. Matousek, M., Schlienger, T., Teufel, S.: Metriken und Konzepte zur Messung der Informationssicherheit. HMD (2004)
30. Pohlmann, N.: Wie wirtschaftlich sind IT-Sicherheitsmaßnahmen. HMD (2006)
31. Mizzi, A.: Return on information security investment-the viability of an anti-spam solution in a wireless environment. International Journal of Network Security 10, 18–24 (2010)
32. Sackmann, S., Syring, A.: Adapted Loss Database–A New Approach to Assess IT Risk in Automated Business Processes. AMCIS 2010 Proceedings (2010)
33. Llanso, T.: CIAM: A data-driven approach for selecting and prioritizing security controls. In: 2012 IEEE International Systems Conference SysCon 2012. IEEE (2012)
34. Chatterjee, S., Sarker, S., Lee, M.J., Xiao, X., Elbanna, A.: A possible conceptualization of the information systems (IS) artifact: A general systems theory perspective 1. Inf Syst J 31, 550–578 (2021)
35. Axelsson, S.: The base-rate fallacy and the difficulty of intrusion detection. ACM Trans. Inf. Syst. Secur. 3, 186–205 (2000)
36. Cavusoglu, H., Raghunathan, S., Cavusoglu, H.: Configuration of and Interaction Between Information Security Technologies: The Case of Firewalls and Intrusion Detection Systems. Information Systems Research 20, 198–217 (2009)
37. Davenport, T.H.: Process Innovation. Reengineering Work Through Information Technology. Harvard Business Press (1993)
38. Magnani, M., Montesi, D.: Computing the Cost of BPMN Diagrams. Technical Report UBLCS-07-17. Bologna (2007)
39. Magnani, M., Montesi, D.: BPMN. How Much Does It Cost? An Incremental Approach. In: Alonso, G., Dadam, P., Rosemann, M. (eds.) Business process management. 5th international conference, BPM 2007, Brisbane, Australia, September 24 - 28, 2007; proceedings, 4714, pp. 80–87. Springer, Berlin (2007)
40. Dijkstra, E.W.: A Note on Two Problems in Connexion with Graphs. Numerische Mathematik 1, 169–271 (1959)
41. Sampathkumaran, P., Wirsing, M.: Computing the Cost of Business Processes. In: Aalst, W., Ginige, A., Kutsche, R.-D., Mayr, H.C., Mylopoulos, J., Sadeh, N.M., Shaw, M.J., Szyperski, C., Yang, J. (eds.) Information Systems: Modeling, De-

velopment, and Integration. Third International United Information Systems Conference, UNISCON 2009, Sydney, Australia, April 21-24, 2009. Proceedings, 20, pp. 178–183. Springer, Berlin, Heidelberg (2009)
42. Sampathkumaran, P.B., Wirsing, M.: Financial Evaluation and Optimization of Business Processes. IJISMD 4, 91–120 (2013)
43. Münstermann, B., Eckhardt, A., Weitzel, T.: The performance impact of business process standardization. Business Process Management Journal 16, 29–56 (2010)
44. Wuellenweber, K., Koenig, W., Beimborn, D., Weitzel, T.: The Impact of Process Standardization on Business Process Outsourcing Success. In: Information Systems Outsourcing, pp. 527–548. Springer, Berlin, Heidelberg (2009)
45. Stöwer, M., Kraft, R.: IT Security Investment and Costing Emphasizing Benefits in Times of Limited Budgets. In: ISSE 2012 Securing Electronic Business Processes, pp. 37–47. Springer Vieweg, Wiesbaden (2012)
46. REIJERS, H., LIMANMANSAR, S.: Best practices in business process redesign: an overview and qualitative evaluation of successful redesign heuristics. Omega 33, 283–306 (2005)
47. Vom Brocke, J., Sonnenberg, C.: Value-Orientation in Business Process Management. In: Handbook on Business Process Management 2, pp. 101–132. Springer, Berlin, Heidelberg (2015)
48. Nurcan, S., Etien, A., Kaabi, R., Zoukar, I., Rolland, C.: A strategy driven business process modelling approach. Business Process Management Journal 11, 628–649 (2005)
49. Chinosi, M., Trombetta, A.: BPMN: An introduction to the standard. Computer Standards & Interfaces 34, 124–134 (2012)
50. Seyffarth, T., Kühnel, S., Sackmann, S.: ConFlex - An Ontology-Based Approach for the Flexible Integration of Controls into Business Processes. Proceedings of the Multikonferenz Wirtschaftsinformatik (MKWI´16), 1341–1352 (2016)
51. Sampemane, G.: Internal access controls. Commun. ACM 58, 62–65 (2015)
52. Sadiq, S., Governatori, G., Namiri, K.: Modeling Control Objectives for Business Process Compliance. Proceedings of the 5th International Conference on Business Process Management (BPM'07), 149–164 (2007)
53. Kühnel, S., Trang, S., Lindner, S.: Conceptualization, Design, and Implementation of EconBPC – A Software Artifact for the Economic Analysis of Business Process Compliance. In: Laender, A.H.F., Pernici, B., Lim, E.-P. (eds.) Conceptual Modeling. 38th International Conference, ER 2019, Salvador, Brazil, November 4–7, 2019, Proceedings, pp. 378–386 (2019)
54. Bhamidipaty, A., Narendra, N.C., Nagar, S., Varshneya, V.K., Vasa, M., Deshwal, C.: Indra: An integrated quantitative system for compliance management for IT service delivery. IBM Journal of Research and Development (IBM J. Res. & Dev.) 53, 1–12 (2009)
55. Doganata, Y.N., Curbera, F.: A method of calculating the cost of reducing the risk exposure of non-compliant process instances. In: Jajodia, S., Kudo, M. (eds.) Proceedings of the first ACM workshop on Information security governance, p. 7. ACM, New York, NY (2009)

56. Abbas, J., Mahmood, H.K., Hussain, F.: Information security management for small and medium size enterprises. Sci. Int. (Lahore) 27, 2393–2398 (2015)
57. Alshboul, Y., Streff, K.: Analyzing Information Security Model for Small-Medium Sized Businesses. AMCIS 2015 Proceedings (2015)
58. Díaz Redondo, R.P., Fernández-Vilas, A., Fernández dos Reis, G.: Security Aspects in Smart Meters: Analysis and Prevention. Sensors 20, 3977 (2020)
59. Chen, Q., Lambright, J., Abdelwahed, S.: Towards Autonomic Security Management of Healthcare Information Systems. 2016 IEEE First International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE), 113–118 (2016)

Analysis of Public Cloud Service Level Agreements – An Evaluation of Leading Software as a Service Providers

Michael Seifert[1]

[1]Martin Luther University Halle-Wittenberg, Chair for Information Management,
Universitaetsring 3, 06108 Halle (Saale), Germany
michael.seifert@wiwi.uni-halle.de

Abstract. Public cloud and software as a service (SaaS) are two of the largest growing IT markets in recent years. Cloud customers need to assess whether the predefined service level agreements (SLAs) of public cloud providers are suitable for their business requirements. Due to the lack of a standard SLA formulation, cloud consumers have significant effort in analyzing SLAs against their compliance, which could be supported by semi-automated SLA management.
SLAs of five leading SaaS providers with comparable public cloud business applications were examined as an as-is analysis. Using 18 derived parameters, the SLAs were formalized and evaluated in terms of matchmaking. The percentage of formalization and matchmaking among the five providers was found to vary between 20% and 73,3% across four SLA categories. Several contributions could be made for practitioners, but also for researchers on how to address the high degree of heterogeneity in public cloud SaaS SLAs.

Keywords: public cloud, software as a service, service level agreements

1 Introduction

The entire cloud market has been increasing continuously for years [1, 2]. Especially the market of public cloud [1] as well as of software as a service (SaaS) [1, 2] is growing significantly. An increasing number of companies are deciding to consume their business applications from the cloud instead of providing them by themselves [3]. At the same time, it enables software vendors to provide their solutions to a wide range of customers [4]. SaaS adoption is receiving increasing attention in practice [5]. The possibility of fast implementation and a higher innovation cycle makes SaaS attractive for businesses [4]. The billing model – from capital expenditure to operational expenditure – is also a valid argument for adopting SaaS in comparison to traditional application service consumption [6].
But cloud providers are also affected by typical IT challenges. For example, cloud providers may require downtime to perform maintenance on their IT infrastructure [7,

16th International Conference on Wirtschaftsinformatik,
March 2021, Essen, Germany

8]. At times, even large cloud providers, and therefore cloud users, experience unplanned downtime [9]. These planned and unplanned downtimes are usually defined and described by cloud providers. This information is agreed and documented with the customer in so-called service level agreements (SLA) [10]. Many cloud providers (usually public cloud providers) even publish their SLAs before signing a contract, which makes it possible for potential customers to analyze them in advance [7, 8].
Accordingly, as a potential cloud customer, an upcoming decision to adopt cloud services should always be based on the customer's own business criticality (e.g. for possible unavailability of the service) to assess risk and service level compliance [11, 12].
The main challenge here is the lack of cloud SLA standards. For potential cloud customers, this means to evaluate the SLA individually against their own business requirements. In addition, certain information that one provider describes in its public SLA may be documented differently, or not at all, by another provider [7].
When evaluating the SLAs of cloud providers on the customer side, it should also be noted that new cloud services often have to be integrated or composed with existing IT services (e.g. for master data exchange) [13, 14]. This means that the cloud customer must not only evaluate the components of the SLA for themselves but aggregate them with SLA parameters of existing IT services to evaluate whether the composition of services continues to meet their business requirements or at least does so at acceptable risk [12, 13].
In research, established models and methods are already proposed for the two scenarios, (I) cloud service selection [15, 16] and (II) cloud service composition [17, 18]. There are also numerous ontologies and meta-models published for standardization and semi-automated SLA-aware selection and composition of cloud services [19, 20]. To enable evaluation and enhancement of models and methods in research, as well as to provide an overview to cloud customers and providers, the state of current cloud SLAs is identified. This study was conducted with the following research questions (RQ), as an as-is analysis of present-day public cloud SaaS SLA.

- RQ1: How can public cloud SaaS SLAs be formalized and categorized in a consistent way?
- RQ2: How much can the formalization of SLA components be used to compare or aggregate (named matchmaking) content from different providers?
- RQ3: What can be derived for research and practice from the results of this study?

To answer these research questions, the next section introduces the fundamental cloud terminology and necessary concepts as a theoretical background. Next, the definition of the study scope is provided by presenting the choice of the study sample and the criteria for analysis. In addition, related work is presented in section 3 and compared with the study scope at hand. Section 4 outlines the data collection of five leading public cloud SaaS provider and their SLAs to make the research comprehensible. Furthermore, the collected data is formalized and categorized here according to RQ1 in context of a moderated focus group as a qualitative research method [21]. In section 5, the five cloud provider SLAs are instantiated according to the formalization. The parameters are then analyzed in terms of their matchmaking to provide an answer to RQ2. The evaluation

and discussion of the analysis in section 6 is followed by a consideration of threats to validity of this research in section 7. The article ends with the conclusion in which the contributions to research and practice of this paper are summarized.

2 Theoretical Background

The study is grounded on cloud terminology following the National Institute of Standards and Technology (NIST). Three cloud service models and four cloud deployment models can be distinguished [22].

The service models are differentiated into Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) [22]. IaaS describes a cloud service in which the provider delivers a complete IT infrastructure ready to use to the consumer [22]. Thereby, computational as well as network and storage resources are composed. With PaaS, further services on top of the composed IT infrastructure are delivered to the customer, enabling application development, for example [22, 23]. With PaaS, customers get the opportunity to develop their own applications in the cloud. With SaaS, usable software is provided to the cloud consumer on top of IT infrastructure [13, 22]. SaaS is usually used by organizations when the cloud application already meets the functional business requirements or when in-house operation of the application is not preferred.

The cloud deployment models are divided into Private Cloud, Public Cloud, Community Cloud, and Hybrid Cloud [22]. Private clouds are services that are deployed by the provider for a specific consumer organization [24]. The private cloud provider is usually in close interaction with the customer in order to consider their business requirements. In contrast, the public cloud is about the provider making the cloud service available to many users and in general [22, 24]. Due to the identical composition, the cloud provider can deliver its service to a large number of customers at the same time. Community cloud is similar to private cloud, but is in contrast provided to be consumed by multiple organizations with similar concerns [22, 24]. Community cloud is used, for example, when several universities consume the same cloud service, but want to have their respective customizing considered. Hybrid cloud is defined as the combination of at least two cloud deployments [22, 24]. The most common type of hybrid cloud is the combination of public cloud and private cloud. The increasingly popular hybrid cloud driven by public cloud SaaS adoption has significant impact on IT management [25].

In order to ensure the contractual relationship between the cloud provider and the customer, service level agreements are signed. A Service Level Agreement (SLA) is a contract for an agreed IT service between a provider and a consumer [10]. The details of the SLA must be underpinned by measurable parameters before and during the service lifecycle in order to be comprehensible for the provider and the customer. To measure and evaluate agreed performance levels of cloud services, qualities of service (QoS) are commonly used [26].

3 Study Scope and Related Work

The study presented in this paper has a two-sided target audience, (I) research and (II) practice. For researchers, the study aims to provide new practical insights for further adaptation and evaluation of existing SLA management models and concepts (e.g. smart contracts), as well as for cloud selection and composition methods and artifacts (e.g. QoS aggregation). For practitioners, the study is of interest because it provides the cloud consumer with an overview of what aspects of public SLA they can align their business needs with. For cloud providers, the analysis serves as a guide to what other providers present in their SLAs and how the survey sample focuses on various SLA parameters and categories.

For the analysis of the SLAs, two evaluation criteria formalization and matchmaking are applied. Formalization is understood as the distillation of the described semantic in the SLA as comparable parameters, as in [7] and [8]. Formalization is therefore where (I) the aspects are included in the respective SLA of the providers and (II) can be assigned to the respective parameters defined.

In order to support the SLA management, we use matchmaking as a second evaluation criteria. Matchmaking is known as a method in QoS-compliant selection of Web services [19]. As an approach to examine constraint satisfaction problems, metrics are checked for semantic and unit-specific equivalence [27]. The SLA parameters are checked by matchmaking to ensure that they are operable among providers, i.e. (I) comparable in terms of cloud service selection or (II) aggregable in terms of cloud service composition.

The study is conducted with focus on one cloud model, namely SaaS. The decision was made because it is expected that IT departments will increasingly need to evaluate SLA compliance in the context of business requirements based on functional or strategic preferences of a specific cloud application [5].

It was also decided to focus on public cloud as the deployment model of the study. Both the decision for the cloud model and the cloud deployment of the study are supported by the high market relevance [1, 2].

Another decision regarding the scope of the study is the focus on business applications (compared to cloud applications for private use). The reason for this is that the commercial risk of insufficient service levels is significantly higher in the business context. In order to ensure the best possible comparability of the SLAs of different providers, business application cloud services were analyzed that are not industry specific.

The scope of the study aims to achieve the highest possible generic coverage, while at the same time ensuring the highest possible transparency of the selection, in order to be able to use the results of the study as broadly and specifically as possible. In the context of the presented study scope, two related work studies are presented in Table 1.

Table 1. related work

	Baset (2012) [7]	Guila and Sood (2013) [8]
title of publication	Cloud SLAs: Present and Future	Comparative Analysis of Present Day Clouds using Service Level Agreements
cloud models	IaaS, PaaS	IaaS, PaaS, SaaS
cloud providers	Amazon, Azure, Rackspace, Terremark, Storm	Rackspace, Engine Yard, Google
SLA parameters	service guarantee, service maintenance, service credit, service violation measurement & reporting	service commitment, definition, credit request/claim, service credit, SLA exclusions

The articles of Baset [7], and Guila and Sood [8] are from the years 2012 and 2013. Due to the passing time in between, it can be assumed that there are changes in the common public cloud SLA. Accordingly, our investigation provides a refresh regarding current cloud SLAs.
In contrast to our fixed scope on SaaS, at least two different cloud models are considered in each of the studies. Both studies also examined public cloud SLAs, so publicly available SLAs served as the foundation.
One issue of criticism in both studies is the comprehensibility of the vendor selection. Neither article explains how the selection is made for each cloud model considered. The article at hand will therefore describe the selection of vendors to be analyzed in section 4 based on the maximum possible generalizability of our results.
Last, this study differs from related work in the depth of analysis. With the motivation of semi-automated processing of the contents of SLA, the capability of matchmaking for the parameters is examined in section 5. The studies by Baset [7], and Guila and Sood [8] each stop at the formalization of the SLA aspects, and thus do not examine subsequent machine processing.

4 Data Collection and SLA Formalization

The data collection starts with a search for market study on the valuation of cloud computing. After screening the two studies on the cloud computing market of Gartner Incorporated (Gartner) [1] and Synergy Research Group (SRG) [2] the leading vendors of SaaS were selected. The selection of our sample for public cloud SaaS business applications goes back to the breakdown of the "Worldwide Market Share of Enterprise SaaS" by SRG [2] and is shown in Table 2.
The cloud services depicted are all public cloud SaaS and, to ensure comprehensibility, non-industry-specific IT applications for business context. Based on the top five enterprise SaaS providers, administrative business applications were selected that could potentially be used in a variety of organizations. Content management systems (CMS) as well as customer relationship management (CRM) and enterprise resource planning (ERP) systems are used in almost all organizations and thus provide a suitable basis for an analysis.

Table 2. selected cloud providers and applications

vendor	application product	application type	links
Adobe	Adobe Experience Manager	Content Management System (CMS)	[31-32]
Microsoft	Microsoft Dynamics 365 Business Central	Enterprise Resource Planning (ERP)	[30]
Oracle	Oracle Fusion Enterprise Resource Planning Cloud	Enterprise Resource Planning (ERP)	[29]
Salesforce	Salesforce Customer 360	Customer Relationship Management (CRM)	[27-28]
SAP	SAP S/4HANA Public Cloud	Enterprise Resource Planning (ERP)	[26]

The data collection process also required further assumptions. First, the formalization of the SLA was performed in each case with reference to corresponding productive system of the cloud service. This represents the aspiration to reflect the business risk in the case of downtimes of the economically relevant systems. Second, in order to formalize certain SLA components, a specific region in which the system is hosted had to be assumed. For this we assumed to be from Germany and chose a region as close to Germany as possible.

The formalization was performed with the following sequence and in context of a moderated focus group [21]. The focus group consisted of 6 researchers and 4 practitioners, each of whom was included in the discussion at both stages of formalization (phase one and phase two).

In phase one, the SLA documents [28–34] were reviewed completely for each of the five providers in sequence and recorded in tabular form for each SLA-relevant parameter. The naming of the tabular documentation of the parameters was inspired by the respective SLA documents and the naming of the parameters of the related work (shown in Table 1). Once an aspect was identified in a subsequent SLA that did not semantically fit into existing parameters, a new parameter was created. Accordingly, the dataset of formalized parameters in Table 3 represents a union of the aspects of the five SLAs. Even if this means that not every parameter can be instantiated or mapped for each of the five SLAs of a provider. Instead, this satisfies the objective of an overview of possible aspects of a present-day public cloud SaaS SLA.

In phase two, after going through all the SLA documents, minor adjustments were made to improve the understandability and comprehensibility of the parameters and categories. For example, the distinction between maintenance and major release upgrades was formulated consistently according to their three relevant aspects. Potential shortcomings in the generation of the formalization are discussed in section 6 with respect to the validity of this study.

As the result, a formalization of SLA corresponding to four categories, each with associated two to six parameters (18 parameters in total), has been generated which is shown in Table 3.

Table 3. formalized SLA parameters and categories

category	no.	parameter	metric, description
service commitment	1.1	target service uptime	percent of minutes per month
	1.2	downtime	definition of downtime
	1.3	exclusion	definition of exclusion from downtime calculation
	1.4	service timetable	time when the service is available
	1.5	recovery time objective (RTO)	maximum time (in hours) between decision to active recovery process and the point at which you may resume operations
	1.6	recovery point objective (RPO)	maximun period (in hours) of data loss from the time the first transaction is lost
service maintenance	2.1	region	where the service is hosted
	2.2	system maintenance announcement	time of announcement of maintenance
	2.3	system maintenance date	maintenance starting time (time zone)
	2.4	system maintenance duration	maximum duration in hours for the maintenance
	2.5	major/release upgrades announcement	time of announcement of the upgrade
	2.6	major/release upgrades date	upgrade starting time (time zone)
	2.7	major/release upgrades duration	maximum duration in hours for the upgrade
service credit	3.1	credit calculation	service credit in relation to monthly payment
	3.2	credit notification	time to report a violation to the provider
	3.3	maximum credit volume	maximum service credit to be paid per month (as a percentage of the monthly fee)
service contract	4.1	termination clause	condition for exceptional termination of the order
	4.2	end of life	notification before the service is no longer generally available (in month)

The first category, *service commitment* (cf. Table 1, Guila and Sood), bundles issues around general availability and possible recovery from failures. *Target service uptime* (1.1) indicates the percentage of minutes the system is available per month. *Downtime* (1.2) specifies what is considered unavailable in terms of billing and *exclusion* (1.3) describes when the provider is exempt from the responsibility of promised uptime. *Service timetable* (1.4) describes the time when the system is up and running, even if no one is working on it. This is relevant, for example, when the system performs scheduled job processing during the night. Last, *recovery time objective (RTO)* (1.5) and *recovery point objective (RPO)* (1.6) are common metrics for the time needed to recover (RTO) and time of maximum data loss (RPO).

Service maintenance (cf. Table 1, Baset) covers the aspects in which the service is planned to be unavailable. This may happen for various reasons. On the one hand, due to necessary *system maintenance* (2.2 - 2.4) on underlying infrastructures or due to *major/release upgrades* of the software to a new release (2.5 - 2.7). The specified parameters are therefore identical for maintenance and upgrades. The *announcement* (2.2, 2.5) indicates the time before the unavailability of the application is announced. The *date* (2.3, 2.6) determines at which time (day and time), according to the stated time zone, the downtime usually takes place. The *duration* (2.4, 2.7) indicates how long the downtime typically lasts from the start time date. The *region* parameter (2.1) is used to specify the location where the service is hosted. This generally has an impact on the scheduled downtimes.

The *service credit* category (cf. Table 1, Guila and Sood, Baset) combines all financial aspects that are relevant once the service fails to fulfill the agreement and the customer receives a fee back. Service *credit calculation* (3.1) indicates how the billing is calculated in relation to the monthly fee for the cloud service. Whereby *maximum credit volume* (3.3) represents the maximum of it. The *credit notification* (3.2) determines the period of time in which the customer is supposed to submit the claim to the provider in order to receive the service credit.
The category *service contract* contains the potential termination of the contract for both parties. The *termination clause* (4.1) defines the number of service level violations after which the customer may terminate the contract for cause. *End of life* (4.2) specifies the period of time in advance for the provider to terminate the cloud service.

5 Evaluation and Discussion

The parameters have been instantiated via the SLA documents of the five providers (see Table 4). The instantiation of the formalization and the capability to be comparable and aggregable (matchmaking) is assessed for all parameters and evaluated across the categories.
With target service uptime it is noticeable that one provider (Salesforce) is not matchable (adjective of matchmaking) because it does not specify a quantitative availability. Downtimes can only be formalized for three vendors and are not matchable there due to the complex wording. The exclusion of availability-reducing factors can be formalized for all vendors. However, the fine details in the SLA are phrased in such a linguistic way that they are not matchable. The service timetable is explicitly described by three out of five providers. However, based on the description of all other parameters, we assume that all providers offer 24/7 service. The formalization of service timetable can therefore be questioned. The formalization of just one provider with regard to the practically highly relevant RTO and RPO documentation is highlighted as potential for improvement in cloud provider practice.
Many cloud providers set planned downtimes depending on the usual business hours per region. For example, these downtimes are usually scheduled for weekends. However, if the cloud service of your choice is not offered in your region, this can lead to scheduled downtimes during the week. Maintenance announcement is only defined for two of the providers. The announcement for upgrades, on the other hand, can be formalized for three providers, but due to vague descriptions it is only matchable for one provider. In this context, matchable means that during the service lifecycle it is possible to check automatically whether maintenance is scheduled by considering the minimum number of days prior notification (as automatically check interval). Maintenance date can be formalized for system maintenance and upgrades in five out of ten potential parameters. All parameters are matchable and give cloud consumers, in combination with maintenance duration, the possibility to compare the potential maintenance windows (which times disrupt their business less) and to aggregate (which maintenance days cover all components of their composite service).

Service credit is almost entirely formalizable across all parameters of four providers. Even the credit calculation of the four different providers is very similar which makes it easily matchable. However, it is noticeable that the maximum credit volume varies significantly (between 10% to 100%). The relevance of this category is considered to be quite high because, in a best-case scenario, the service credit should be able to compensate for the loss caused by business interruption as risk transfer.

Table 4. instantiated formalization and matchmaking of the cloud provider sample

cat.	no.	Adobe	Oracle	Microsoft	Salesforce	SAP
service commitment	1.1	99,9	99,9	99,9	commercially reasonable efforts to make the services available 24/7	99,5
	1.2	service not available to the customer, except any excluded minutes	-	users unable to login (excluded planned downtimes)	-	minutes the system is not available (excluded downtimes)
	1.3	misbehavior of customer	scheduled downtimes from my oracle support	planned downtimes; list of limitations (e.g. networt, inappropriate usage)	planned downtime; circumstances beyond reasonable control	regular maintenance, major upgrades; out of provider control
	1.4	24/7	-	-	24/7	24/7
	1.5	-	12	-	-	-
	1.6	-	1	-	-	-
service maintenance	2.1	America	-	EMEA	EU	Europe
	2.2	-	-	notified at least five business days in advance	ten days prior to the maintenance	-
	2.3	-	-	22:00 (UTC)	SAT, 22:00 (UTC)	SAT, 22:00 (UTC)
	2.4	-	-	8	4	4
	2.5	-	-	choose a specific weekend	approximately one year before the release date	notified at least five business days in advance
	2.6	-	-	-	FRI, 22:00 (UTC)	SAT, 4:00 (UTC)
	2.7	-	-	3 hours	6 hours	24 hours
service credit	3.1	<99,9% -> 5% fee, <99,5% -> 10% fee, <95% -> 15% fee, <90% -> 25% fee	per 1% below availability (99,9) you get 2% credit of your monthly fee; service credit is paid with the second month of missed service availability in a six month period	<99,9% -> 25% credit, <99% -> 50% credit, <95% -> 100% credit	-	per 1% below availability (99,5) you get 2% credit of your monthly fee
	3.2	-	30	within two months of the end of the billing month in which the incident occurred	-	30
	3.3	25	10	100	-	100
service contract	4.1	-	availability violation for three consecutive months	-	-	-
	4.2	-	12	-	-	-

formalizable	matchable

Service contract can be formalized by one provider and is matchable with parameters of other providers. Again, relevant aspects of the SLA are mapped, which could be used for enrichment in the SLA of other providers.

In order to get an overview of the results of the analysis, the assigned labels in Table 4 (formalizable, matchable) were evaluated quantitatively. The result of this analysis can be seen in Table 5 and are discussed in the following.

Service commitment is often not trivial to process by machine due to the lack of formalizability, which is seen as a challenge and a risk for cloud consumers. In addition, even if it can be formalized, it is often difficult to compare or aggregate it due to over-defined terminology and exclusion (see 1.2, 1.3 Table 4).

Service maintenance formalizability is basically enabled by three out of five providers. The formalized parameters allow a suitable processing in general. It remains to be said

that both practice and research in the discovery or decision phase must nevertheless reckon with uncertainty in the run-up to the announcement or even the lack of announcement of maintenance. Maintenance must therefore be formalizable, measurable and adaptable in later phases of the service level lifecycle.

Table 5. evaluation of formalization and matchmaking of the cloud provider sample

category	formalization	matchmaking
service commitment	60,0%	30,0%
service maintenance	57,1%	40,0%
service credit	73,3%	73,3%
service contract	20,0%	20,0%

Service credit formalizability and matchmaking has the highest percentage of all categories. This shows that the calculation methods are similar across four depicting providers and are therefore easy to process. Nevertheless, it remains interesting for practice and research to include the maximum loss payment in the risk consideration when deciding on the selection of an SLA.
Service contract formalizability and matchmaking is limited to one provider. For the service contract, analogous to the service credit, the challenge for both practice and research is to consider it in the risk management of the cloud application decision.

6 Threats to Validity

To demonstrate rigor and encourage further research, the threats of validity of this study are discussed. Threats of validity are considered in terms of internal validity and external validity.
Internal validity refers specifically to whether an experimental treatment or condition makes a difference to the outcome or not, and whether there is sufficient evidence to substantiate the claim [35]. The following internal validity threats for this study were identified and should be considered for interpretation or further research.

- Insufficient or improper SLA documents or information were collected by the formalization procedure. Accordingly, it may be that the scores calculated for the categories may be inaccurate.
- The selected sample of leading public cloud SaaS providers is chosen biased or is insufficient. Potentially, adding more providers improves calculated category scores and leads to more underrepresented parameters.
- The interpretation of the descriptions or the order of importance in the SLAs was inaccurate or wrong. Our focus group was set up to evaluate the formalization; another group may possibly come to different results.
- The evaluation of the matchmaking of the parameters was performed with the knowledge of existing methods in SLA management. The actual applicability of the labeled parameters is nevertheless to be verified in each case. The evaluation of SLA

management artifacts with the identified parameters is a promising field for further research.
- The survey is statically time-based, so changes in SLAs over time can lead to other results.

External validity refers specifically to whether the results can be considered in real-world environment [35]. The following external validity threats for this study were identified and should be considered for interpretation or further research.

- It is possible that (1.) agreements besides the SLA between provider and customer are made or (2.) further contractual documents affect the consideration.
- The generalization of our identified formalizability and matchmaking can be challenged due to different requirements of the different application types.

7 Conclusion

In this study, based on the motivation of an as-is analysis, five present-day public cloud SaaS SLAs were analyzed in the context of service level compliance and risk management. The study focus was intentionally set on (I) public cloud, (II) SaaS and (III) business-critical applications in order to address the relevance of downtime-related breakdowns in business processes.
With the help of four derived SLA categories and 18 underlying SLA parameters, a general formalizability (concerning at least one provider) was determined. Across the four different categories, formalizability was found to range from an average 20% to 73.3% across the entire sample (concerning RQ1). The high variance in formalizability confirms the common assumption of the lack of SLA standards in practice.
To enable semi-automated SLA management, all parameters were evaluated for matchmaking (comparable and aggregable). Across the four different categories, matchmaking was found to range from an average of 20% to 73.3% across the entire sample (concerning RQ2). Matchmaking has high importance in the context of IT-supported SLA management, and is threatened especially due to low rates (20%, 30% and 40%) in three out of four categories. The emerging deficit can be closed on the one hand (I) by further analysis of matchmaking or (II) by an additional manual evaluation step of potential cloud customers.
An extract of contributions to research and practice elaborated in section 5 are finally summarized (concerning RQ3).

- Practitioners get an understanding of common and uncommon public cloud SaaS SLA parameters and categories to analyze risk and service level compliance prior to an adoption.
- It is also possible for practitioners to identify SLA aspects that may have a high economic importance (e.g. RPO, RTO, planned downtimes) but may not be offered by all providers.

- Researchers get an up-to-date view of SLA parameters that SLA management methods and concepts must take into consideration in order to be applicable to present-day clouds (e.g. temporal logic for downtime aggregation).
- Researchers should consider how business-critical SLA parameters (e.g., service credit calculation and downtime exclusion) can be reflected in terms of risk assessment extending traditional QoS aggregation (e.g., availability multiplication).

References

1. Gartner Inc.: Proportion of Enterprise IT Spending on Public Cloud Computing Continues to Increase, https://www.gartner.com/en/newsroom/press-releases/2020-11-17-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-grow-18-percent-in-2021 (Accessed: 12.01.2021)
2. Synergy Research Group: Quarterly SaaS Spending Reaches $20 billion as Microsoft Extends its Market Leadership, https://www.srgresearch.com/articles/quarterly-saas-spending-reaches-20-billion-microsoft-extends-its-market-leadership (Accessed: 12.01.2021)
3. B. Link: Considering the Company's Characteristics in Choosing between SaaS vs. On-Premise-ERPs. In: Wirtschaftsinformatik (2013)
4. Bennett, K., Munro, M., Gold, N., Layzell, P., Budgen, D., Brereton, P.: An Architectural model for service-based software with ultra rapid evolution. In: Proceedings, IEEE International Conference on Software Maintenance. Systems and software evolution in the era of the Internet : Florence, Italy, 7-9 November, 2001. IEEE Computer Society, Los Alamitos, Calif. (2001)
5. Benlian, A., Hess, T., Buxmann, P.: Drivers of SaaS-Adoption – An Empirical Study of Different Application Types. Bus. Inf. Syst. Eng. 1, 357–369 (2009)
6. M. Janssen, Anton Joha: Challenges for adopting cloud-based software as a service (saas) in the public sector. In: ECIS (2011)
7. Baset, S.A.: Cloud SLAs: Present and Future. SIGOPS Oper. Syst. Rev. 46, 57–66 (2012)
8. Gulia, P., Sood, S.: Comparative Analysis of Present Day Clouds using Service Level Agreements. IJCA 71, 1–8 (2013)
9. Paquette, S., Jaeger, P.T., Wilson, S.C.: Identifying the security risks associated with governmental use of cloud computing. Government Information Quarterly 27, 245–253 (2010)
10. Patel, P., Ranabahu, A.H., Sheth, A.P.: Service Level Agreement in Cloud Computing. Kno.e.sis Publications, THE OHIO CENTER OF EXCELLENCE IN KNOWLEDGE-ENABLED COMPUTING, 1–10 (2009)
11. P. Hoberg, J. Wollersheim, H. Krcmar: The Business Perspective on Cloud Computing - A Literature Review of Research on Cloud Computing. In: AMCIS (2012)
12. Seifert, M., Kühnel, S.: "HySLAC"– A Conceptual Model for Service Level Agreement Compliance in Hybrid Cloud Architectures. Proceedings of the 50th

Annual Conference of the German Informatics Society, Lecture Notes in Informatics (LNI), 195–208 (2021)
13. Sun, W., Zhang, X., Guo, C.J., Sun, P., Su, H.: Software as a Service: Configuration and Customization Perspectives. In: 2008 IEEE Congress on Services Part II (services-2 2008), pp. 18–25. IEEE (2008 - 2008)
14. Andreas Jede, Frank Teuteberg: Understanding Socio-Technical Impacts Arising from Software-as-a-Service Usage in Companies. Bus Inf Syst Eng 58, 161–176 (2016)
15. Kritikos, K., Plexousakis, D.: Requirements for QoS-Based Web Service Description and Discovery. IEEE Trans. Serv. Comput. 2, 320–337 (2009)
16. Vakili, A., Navimipour, N.J.: Comprehensive and systematic review of the service composition mechanisms in the cloud environments. Journal of Network and Computer Applications 81, 24–36 (2017)
17. L. Qi, W. Dou, X. Zhang, J. Chen: A QoS-aware composition method supporting cross-platform service invocation in cloud environment. J. Comput. Syst. Sci. 78, 1316–1329 (2012)
18. Xin Zhao, Liwei Shen, Xin Peng, Wenyun Zhao: Toward SLA-constrained service composition: An approach based on a fuzzy linguistic preference model and an evolutionary algorithm. Information Sciences 316, 370–396 (2015)
19. Kritikos, K., Plexousakis, D., Plebani, P.: Semantic SLAs for Services with Q-SLA. Procedia Computer Science 97, 24–33 (2016)
20. Labidi, T., Mtibaa, A., Brabra, H.: CSLAOnto: A Comprehensive Ontological SLA Model in Cloud Computing. J Data Semant 5, 179–193 (2016)
21. Morgan, D.: Focus Groups as Qualitative Research. SAGE Publications, Inc, 2455 Teller Road, Thousand Oaks California 91320 United States of America (1997)
22. Mell, P.M., Grance, T.: The NIST definition of cloud computing. National Institute of Standards and Technology, Gaithersburg, MD (2011)
23. Yangui, S., Ravindran, P., Bibani, O., Glitho, R.H., Ben Hadj-Alouane, N., Morrow, M.J., Polakos, P.A.: A platform as-a-service for hybrid cloud/fog environments. In: IEEE LANMAN 2016. The 22nd IEEE International Symposium on Local and Metropolitan Area Networks, June 13-15, 2016, Rome, Italy, pp. 1–7. IEEE, Piscataway, NJ (2016)
24. Goyal, S.: Public vs Private vs Hybrid vs Community - Cloud Computing: A Critical Review. IJCNIS 6, 20–29 (2014)
25. Breiter, G., Naik, V.K.: A Framework for Controlling and Managing Hybrid Cloud Service Integration. In: Campbell, R. (ed.) 2013 IEEE International Conference on Cloud Engineering (IC2E). 25 - 27 March 2013, San Francisco Bay, California, pp. 217–224. IEEE, Piscataway, NJ (2013)
26. Suakanto, S., Supangkat, S.H., Suhardi, Saragih, R.: Performance Measurement of Cloud Computing Services (2012)
27. Kritikos, K., Plexousakis, D.: Semantic QoS Metric Matching. In: Bernstein, A., Gschwind, T., Zimmermann, W. (eds.) 4th European Conference on Web Services, 2006. ECOWS '06 ; 4 - 6 December 2006, Zurich, Switzerland. IEEE Computer Society, Los Alamitos, Calif. [u.a.] (2006)

28. Adobe Inc.: Service Level Agreement, https://www.adobe.com/content/dam/cc/en/legal/terms/enterprise/pdfs/MasterSLA-2016DEC5.pdf
29. Adobe Inc.: Service Level Exhibit - AEM as a Cloud Service, https://www.adobe.com/content/dam/cc/en/legal/terms/enterprise/pdfs/SLAExhibit-AEMCloudService-2019DEC12.pdf (Accessed: 12.01.2021)
30. Microsoft Corporation: Service Level Agreement for Microsoft Online Services, https://www.microsoftvolumelicensing.com/Downloader.aspx?documenttype=OSCS&lang=English (Accessed: 12.01.2021)
31. Oracle Corporation: Oracle SaaS Public Cloud Services-Pillar Document, https://www.oracle.com/assets/saas-public-cloud-services-pillar-3610529.pdf (Accessed: 12.01.2021)
32. Salesforce Inc.: Master Subscription Agreement, https://c1.sfdcstatic.com/content/dam/web/en_us/www/documents/legal/salesforce_MSA.pdf (Accessed: 12.01.2021)
33. Salesforce Inc.: Preferred Salesforce Maintenance Schedule, https://help.salesforce.com/articleView?id=000331027&type=1&mode=1 (Accessed: 12.01.2021)
34. SAP SE: Service Level Agreement for SAP Cloud Services, https://assets.cdn.sap.com/agreements/product-use-and-support-terms/cls/en/service-level-agreement-for-sap-cloud-services-english-v7-2020.pdf (Accessed: 12.01.2021)
35. J. Siegmund, N. Siegmund, S. Apel: Views on Internal and External Validity in Empirical Software Engineering. In: 2015 IEEE/ACM 37th IEEE International Conference on Software Engineering, pp. 9–19 (2015)

Software Compliance in Different Industries: A Systematic Literature Review

Mohammed Mubarkoot[1], Jörn Altmann[1]

[1]Technology Management, Economics and Policy, Seoul National University, Seoul, Korea
mubarkoot@snu.ac.kr, jorn.altmann@acm.org

Abstract. With the emergence of new software development paradigms (e.g., distributed teams and crowd-sourcing), the software supply chain became more complicated than ever. This, in turn, raises concerns in software compliance in many industries, as ensuring adherence beyond functional requirements is very critical. This paper uses a systematic literature review, to investigate the frameworks used for managing compliance of software and software services and their applications across different industries. The review also looked into industry-specific software compliance requirements. A total of 156 primary studies have been collected, of which 63 studies match the criteria indicated in the review protocol. The study develops a classification of these frameworks based on industry-specific needs, business requirements, and the context of compliance. Findings of this research help researchers and practitioners to identify important aspects of software compliance and set directions for future research and development.

Keywords: Software Compliance, Policy, Regulations, Industry Requirements, Systematic Literature Review

1 Introduction

Complex software applications evolve over time and tend to diverge from the intended or documented design models. This deviation makes the system hard to understand, modify, and maintain in the long run [1]. Nevertheless, modifications and updates of software systems are inevitable, in order to respond to changes in business requirements. Nowadays, software development happens globally across geographically distributed and autonomous teams consuming huge amounts of software components drawn from a variety of different sources [14] [75]. Although this helps organizations to deal with technical and economic challenges, it is also increasing unintended risks [2]. These include manageability [1], traceability and auditing [3], adherence to policies and service level agreements (SLAs) [4] [77], service availability [5], security vulnerabilities [2] and use of non-compliant components [3]. Moreover, risks can arise when failing to comply with policies, regulations and industry standards, which is highly critical to not only business continuity [6] but also other consequences that result from non-compliance including cost of litigation and loss of reputation to mention a few. Moreover, typically, whenever the complexity of a software increases, its quality decreases [7] [76].

16th International Conference on Wirtschaftsinformatik,
March 2021, Essen, Germany

Software applications and services should be built in accordance (or compliance) to various policies, best practices, industry-specific needs, and regulations [2]. For most common practices nowadays, ensuring policies adherence to compliance requirements is often held by compliance experts, which is time-consuming and error-prone. What also complicates this process is the gap between compliance experts and domain experts. Eventually, management and monitoring of application behavior become more complicated over time [6]. Typically, requirements are extracted from legal regulations, branch-specific guidelines, internal code of conduct, and other sources. However, challenges arise from the change of these requirements as well as the adaptive environments along with rapid technological changes [9].

Furthermore, in the software supply chain, the philosophy of "assemble more, code less" is becoming very common nowadays, leading to issues in governance, risk management, and compliance (GRC) [2]. Therefore, with modern software applications and services that consist of complex and heterogeneous components, it becomes more challenging to manage their compliance to internal business policies, external regulations, industry standards, infrastructure and security requirements. The task becomes even more complicated, when different deployment technologies are used, in which the alternative manual way of checking and matching compliance requirements tend to be highly risky and mistakes are likely to happen [10]. Moreover, Nick [11] raised an issue with the control problem related to the advances in the capabilities of artificial intelligence (AI) in that self-optimizing AI components can misbehave and go against the boundaries of policies or regulations. All these challenges make the manual way of auditing and checking software compliance useless calling for a more innovative way to check software compliance.

The main objective of this systematic literature review is to survey the existing frameworks used for compliance checking of software and software services, their industry of application and compliance requirements for each industry. The contribution of this research is that it highlights recent progress in the compliance management of software and software services and that it points to future research areas.

Subsequent sections of this paper are organized as follows. Section 2 presents the methodology used, including the research questions formulated and the details on the review protocol used to execute this research. Section 3 presents the analysis and findings of the review. Section 4 discusses the findings and draws directions for future research. Finally, the conclusion section wraps up the key points of the review.

2 Methodology

We based the methodology for conducting a systematic literature review (SLR) on the one of Kitchenham at al. [12], which is one of the more relevant methods in the field of information systems research. We formulated the research questions and, then, developed and validated the review protocol. Afterwards, the collected studies were screened to add those, which are more relevant to our database. After that, we applied a set of criteria for inclusion and quality assessment. Then, after the data is extracted, documented into a database, and analyzed, the results are synthesized. Finally, findings

are discussed and mapped against the research questions. The following subsections briefly discuss the research questions and the review protocol.

2.1 Research Questions

There are many aspects to investigate in the area of software compliance. However, we limit our review objective to surveying existing frameworks, their applications in industries, and compliance requirements by each industry. Therefore, we aim at answering the following two research questions:

RQ1. What are the existing frameworks of software compliance management and their applications in industries?

RQ2. What are the compliance requirements and needs of each industry?

2.2 Review Protocol

After setting up the research questions, we developed the review protocol, which includes the strategy applied for searching, selecting, including, and assessing the primary studies. We conducted a manual search using the terms "Software AND Compliance" to retrieve relevant studies. The search process considers the matches of both keywords in the title, abstract, or keywords of scholarly articles.

Selection of Sources: To ensure that the review includes as many relevant studies as possible within the defined search terms, we conducted a manual search in the following sources: *IEEE Xplore, ACM Digital Library, MDPI, Elsevier, HeinOnline, Springer, Web of Science, Scopus and Google Scholar.*

Inclusion Criteria: To keep our review focused on the objectives stated in Section 2.1, we developed a set of inclusion criteria as part of the review protocol. Therefore, the following criteria are applied to include primary studies for the final review:

Criterion 1: Only primary studies published between 2010 and 2020 are included.

Criterion 2: Relevant studies are only included for the review. By this, we mean studies that contribute to addressing our research questions.

Criterion 3: Only studies, which are accessible through Google Scholar and Seoul National University library, considered for the review.

Criterion 4: Only studies written in English are included for the review.

Criterion 5: Studies included for the review are limited to journal publications, conference proceedings, workshop proceedings, and symposium proceedings. Secondary studies, book chapters, presentations, dissertations, and reports are excluded.

Data Extraction: We used Zotero version 5 as a referencing tool to document, manage, and organize the references of the retrieved studies. We also set up a database, to record and extract relevant content. For that purpose, we used Microsoft Excel 2019, to record and manage findings. This helped making the analyses and investigations of findings simpler. It also provides a reference for further investigations in a systematic way.

3 Analysis of Results

3.1 Descriptive Analysis

Initial search on Google Scholar found 253 scholarly articles. We conducted an initial screening to eliminate irrelevant articles. From that, a total of 156 studies have been collected with respect to the search terms indicated in Section 2. Then, after applying the inclusion criteria, which are indicated in the review protocol, and checking the relevance of the primary studies to the research questions, only 63 primary studies are left for the review. Table 1 shows a summary of the studies selected for the review, including the database and types of studies. The table shows that more than half of the primary studies are conference papers. The rest are journal publications or proceedings from symposia and workshops. From well-known scientific databases, including IEEE, Elsevier, HeinOnline, ACM Digital Library, Springer and CiteSeerX, a total of 47 studies were collected. The remaining 16 studies are from sources other than the abovementioned databases, which include universities journals and proceedings.

Table 1. Summary of Selected Papers

Scientific Database	*Total Number of Papers*	*Journals*	*Conferences*	*Symposium*	*Workshops*
IEEE	29	1	24	2	2
Elsevier	5	5	-	-	-
HeinOnline	2	2	-	-	-
ACM Digital Library	5	-	2	2	1
Springer	5	2	3	-	-
CiteSeerX	1	1	-	-	-
Others	16	7	9	-	-
Total	63	18	38	4	3

Figure 1 shows the distribution of the publication years of the primary studies between 2010 and 2020 as indicated in the protocol of this review (Section 2). The trend in Figure 1 indicates that the research in software compliance is still growing, which is an indicator of the growing importance of the field.

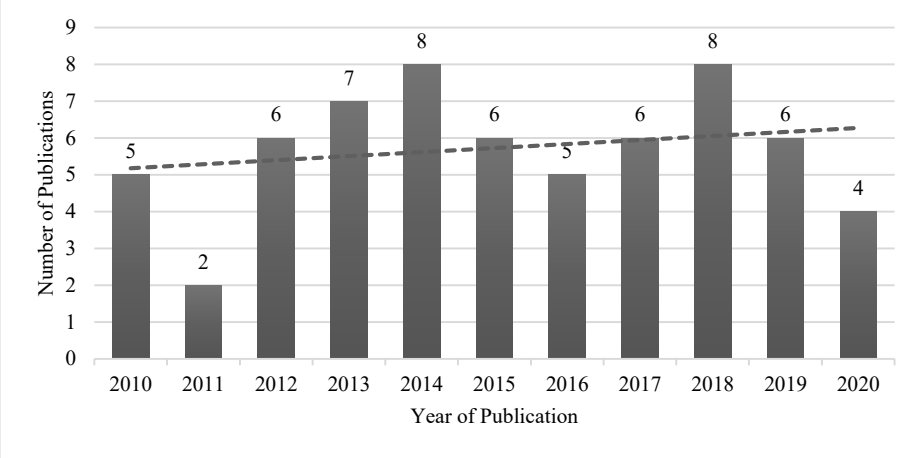


Figure 1. Distribution of Selected Papers by Year of Publication

3.2 Industry Requirements and Compliance Frameworks

Figure 2 summarizes the software compliance applications by industry. The analysis found that certain industries are investigated more than others. In the software industry itself, the review found 36% of the primary studies discuss compliance concerns in the software field. Then, the cloud industry comes with 22% of the studies, followed by the healthcare, in which 13% of the primary studies address issues related to software compliance. The figure also shows that 14% of the studies did not specify the industry of application. The rest of the industries which are discussed by fewer studies are as follows: manufacturing (6%), automobile (2%), financial (3%), aviation (2%), and e-government (2%). Some of the primary studies discuss a certain industry in the context of clouds (e.g., financial software running on clouds). For such scenarios, we classify them to their original industry. In other words, if a study discusses compliance of financial software on clouds, then we consider the focus to be on the financial industry.

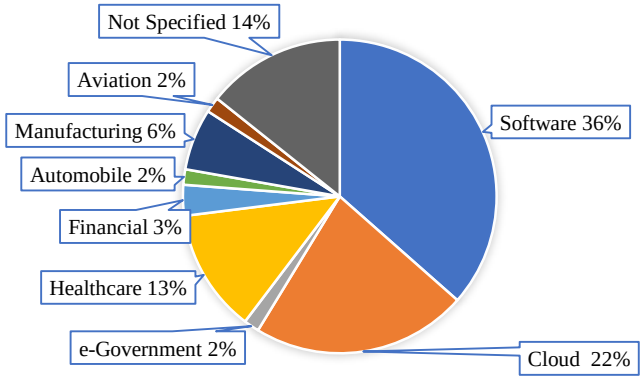


Figure 2. Distribution of primary studies by industry of application

Figure 2 also reflects the amount of challenges that each industry deals with. The majority of primary studies discuss compliance concerns related to software and cloud industries. This indicates that there are a lot of challenges and solutions discussed for these industries. The reason could be that these two industries are highly dynamic and many of their resources are available. Besides that, software and cloud industries are the central discussion in many of the primary studies. Nevertheless, changes in policies, regulations, and requirements are inevitable in every industry. The reviewed studies only discuss industries illustrated in Figure 2. Other industries are not found in primary studies based on our search terms. Perhaps, different terms are used, which do not include any of the search terms specified in our protocol.

To give a detailed picture on compliance requirements given by each industry, Table 2 shows the applications of compliance frameworks in the different industries along with the requirements needed by each industry. In the software industry, primary studies focus on compliance concerns related to distributed teams, intellectual property, components licensing, copyrights, reliability, security, trust, auditing, user permission, general data protection regulations (GDPR), privacy, software development lifecycle (SDLC), software design, regulatory requirements, process compliance, maintenance, governance risk & compliance (GRC), transparency, design-code compliance, and accountability. In the cloud industry, we found that studies focus on concerns related to security, privacy, compliance to service level agreements (SLA), trust, adaptation, accountability, resilience, application development, application deployment, management, provisioning, and adherence to regulations. Table 2 also shows that there is little attention to software compliance in governments, especially no attention on interoperability concerns of e-government services. Healthcare is an industry, which gained attention by primary studies. According to the primary study, we found that software systems need to comply with the health information technology for economic and clinical health (HITECH), health insurance portability and accountability (HIPAA), personal health information protection (PHIPA), organization for economic co-operation and development (OECD), requirement engineering, safety-critical aspects, quality, and reliability.

Moving to more safety-critical industries like automobile, manufacturing, and aviation, we found that these industries share some common compliance requirements, including reliability and compliance to safety standards. In addition to reliability and safety requirements, primary studies also show that the manufacturing industry focuses also on concerns including security, deployment & provisioning, privacy, GDPR, and industrial automation. Finally, the rest of primary studies did not specify or target a certain industry, however, those studies focus on compliance issues related to software design, service-oriented architecture (SOA), legal contracts, distributed systems, flexibility, auditing, transparency, security, IT service management (ITSM), business process modeling (BPM), outsourcing, and GRC.

Table 2. Compliance framework applications and compliance requirements in different industries

Industry	*Compliance Requirements*	*Reference*
Software	Distributed teams, intellectual property, components licensing, copyrights, reliability, security, trust, auditing, user permission, GDPR, privacy, SDLC, software design, regulatory requirements, process compliance, maintenance, GRC, transparency, design-code compliance, accountability	Singi et al. [14], Yun et al. [13], Singi et al. [2], van der Burg et al. [15], Hemel et al. [31], German and Di Penta [32], Jeff and Alan [33], Koltun [34], Von Willebrand and Patanen [35], Subramaniam and Natarajan [42], R P et al. [49], Gangadharan et al. [53], Hamou-Lhadj [55], Truong and Nguyen [56], Jensen et al. [58], Marques and Cunha [59], Arogundade et al. [62], Engiel et al. [63], Savarimuthu et al. [65], Chakraborty and Chaki [66], Jorshari and Tawil [67], Vytautas and Friedrich [70], Ozbas-Caglayan and Dogru [72],
Cloud	Security, privacy, SLA, trust, adaptation, accountability, resilience, application development, application deployment, management, provisioning, adherence to regulations, distributed services, SOA	McCarthy et al. [16], Suneel and Guruprasad [17], Hashmi et al. [18], Brandic et al. [36], García-Galán et al. [39], Florian et al. [40], Faniyi and Bahsoon [41], Singh and Sidhu [44], Krieger et al. [45], Carrasco et al. [46], Qanbari et al. [47], Breitenbucher et al. [50], Foster et al. [37], Koetter et al. [48]
e-Government	Interoperability	González and Ruggia [19]
Healthcare	HITECH, HIPAA, PHIPA, OECD, requirement engineering, safety-critical systems, quality, reliability	Gardazi and Ali [20], Sartoli et al. [21], Li et al. [22], Ingolfo et al. [51], Khan and Yun Bai [54], Lepmets et al. [64], Zema et al. [68], Maxwell and Antón [74]
Financial	Transparency, accountability, control, response to change	Magnusson and Chou [73], Koetter et al. [28]
Automobile	Functional safety, reliability	Hocking et al. [69]
Manufacturing	Security, deployment and provisioning, safety standards, privacy, GDPR, industrial automation	Zimmermann et al. [23], Castellanos Ardila and Gallina [43], Kittmann et al. [60], Moyon et al. [61]
Aviation	Safety standards, reliability	Jurnečka et al. [71]

Industry	*Compliance Requirements*	*Reference*
Not Specified	Software design, SOA, legal contracts, flexibility, auditing, transparency, security, ITSM, BPM, outsourcing, GRC, reliability	Fischer et al. [24], Tran et al. [25], Sharifi et al. [26], Loreti et al. [27], Groefsema and van Beest [29], Ingle et al. [30], Correia and Brito e Abreu [38], Thalmann et al. [52], Elhasnaoui et al. [57]

4 Discussion

Many industries heavily rely on software and software services, to automate as many of their business processes as possible. Thus, the use of software and software services becomes inevitable in many industries. With that, however, software projects grow and evolve over time as a response to changes in business and industry needs. This, in turn, has a negative impact on software quality according to the theory of software evolution, which was introduced by Lehman [7] in 1980. While most of this is related to functional requirements, there are also non-functional requirements, in which software and information systems need to comply with. These include security, privacy, licensing, reliability, provisioning, interoperability, data sharing, and adherence to regulations. Priorities of such requirements are also different between industries due to the different needs of each industry. The challenges come in fulfilling industry-specific compliance requirements and enable a degree of flexibility to respond to changes as well as checking whether new changes are reflected and enforced at the software level.

The analysis shows that primary studies discussed software compliance frameworks of 8 industries: software, cloud, e-Government, healthcare, financial, automobile, manufacturing, and aviation. Some further studies did not specify the industry, in which their proposed frameworks could be applied. There are some differences among the frameworks proposed by primary studies. These differences are driven by peculiarities of each industry, since each industry has its own business objectives, priorities, compliance requirements, and industry-specific needs. Moreover, the difference between the proposed frameworks is also influenced by the authors' assumptions and the context of compliance that they consider for their framework proposal. Nevertheless, some industries tend to have some compliance needs in common. For example, the manufacturing industry tends to focus on reliability and safety standards, which are also the focus of the automobile and aviation industries. The healthcare industry, however, tends to have different priorities, because they need to meet certain government regulations on healthcare. Furthermore, we found some differences in compliance requirements within the same industry. On top of these, regional-specific compliance requirements add another layer of complexity, especially for globally distributed software services and components.

Referring back to our research questions, there are many frameworks introduced by primary studies according to the analysis. Each has its own peculiarities depending on its application in a certain industry, business requirements, and assumptions considered by authors. In general, there are common issues that the primary studies try to address.

These are the changes in requirements and policies, the gap between IT and laws, the challenge of modeling policies and regulations, and reflecting those changes at a software level. Based on the analysis, compliance requirements, which are discussed most frequently in many industries, are: reliability, safety, security, and privacy, indicating that these requirements are highly critical to most industries.

In the software industry, Singi et al. [14] introduced a framework, in order to help establishing transparency and trust in distributed teams in global software delivery using blockchain. In the same context, other studies also investigated the challenges in crowd sourcing and how the software supply chain is affected in distributed software delivery [2] [25] [27]. Hamou-Lhadj [55] introduced the concept "software compliance engineering", emphasizing that regulatory compliance should be one of the key quality attributes of software products. Jorshari and Tawil [67] also support this argument of including compliance requirement analysis during the software development process, in order to have better governance, risk management and compliance (GRC). Another important aspect of software compliance is software licensing, in which many authors call for checking license compatibility, validation, awareness, dependency check of components, as well as license requirement analysis [15] [31] [32] [33] [35] [53]. The last important compliance issue to emphasize is ensuring design-code compliance. For this matter, Ozbas-Caglayan and Dogru [72] proposed an approach for analyzing software to check the compliance level of design and code using text mining and software repository analysis. To a great extent, the software industry deals with software compliance requirements and concerns from the perspective of software development practices. The aim is to ensure transparency and trust of distributed teams, component licensing, security, privacy, design-code compliance, and process compliance.

The cloud industry has also an increasing concern on compliance issues, especially security and trust between the cloud service providers and service consumers [16] [17] [18]. For this, Suneel and Guruprasad [17] introduced an approach to monitor SLA compliance of a cloud service provider (CSP), which can be implemented at the client end. They assume that a CSP is likely to violate the SLA, spoof the properties of the services, and, then, deliver the services with lower properties. Other studies also try to address the issues of trust, including Florian et al. [40], Singh and Sidhu [44], and Brandic et al. [36]. One of the major challenges in software compliance is modeling policies and legal aspects and enforcing them. For that, Breitenbucher et al. [50] proposed a policy-aware management framework. The framework enables automated provisioning and management of composite cloud applications based on a set of non-functional requirements defined by policies. However, this needs skills of both compliance and domain expertise. To simplify this, Hashmi et al. [18] introduced "security as a service" as a business model. It allows the delivery of managed security services to the user as a cloud service, to provide the end-users with monitoring information on their transaction and, thus, reducing the effect of security concerns. For the same reason, McCarthy et al. [16] introduced "compliance as a service" architecture, which is a cloud brokerage remediation service that checks non-functional security and compliance requirements. They aim at bridging the gap between agility and security, stating that the use of cloud does not guarantee security and legal

compliance, which are still the user's obligation. Lastly, when it comes to service provisioning, automated installation of systems, and checking deployment rules, Krieger et al. [45] proposed an approach that enables modeling of reusable deployment compliance rules. Such rules are executed automatically to check declarative deployment models at design time. In the same context but for highly portable and provider-independent cloud applications, Carrasco et al. [46] introduced a model that supports applications, whose components are deployed on different providers. This, in turn, reduces the issues of portability, interoperability, and vendor lock-in. Overall, the software compliance in the cloud industry has similarities with the software industry, however, the cloud takes slightly higher level focusing on compliance concerns related to management and provisioning of software services, (e.g., security, privacy, service level agreement (SLA), adaptation, resilience, application deployment, distributed services).

In the healthcare industry, software projects also encounter many regulatory challenges, in particular, with respect to privacy of personal data. There is a gap between compliance and software architecture [20]. The evolving regulatory requirements affect all phases of the software development life cycle (SDLC), while in most software development practices, ensuring compliance is performed at requirement level. To bridge such a gap, Gardazi and Ali [20] introduced a compliance-driven software architecture based on a set of information security regulations and non-functional requirements. This helps achieving a compliance-aware software architecture. The majority of primary studies focus on security and privacy requirements represented by HITECH, HIPAA, PHIPA, and OECD. In this regard, and with the growing trend of home-based healthcare services, new compliance challenges have been raised in data collection, transferring, and sharing due to the geographical distribution of patients and their care providers. To address this issue, Li et al. [22] introduced the "CareNet" framework that bridges the gap between availability of software-defined infrastructure and compliance with regulatory requirements of a heterogeneous home-edge-core cloud for the home-based healthcare services. Further frameworks also attempt to bridge the gap between compliance and software architecture, by capturing the variability from legal sources and operating environments, real-time response, and modeling legal rules [20] [21] [74]. The growing development of smart healthcare services is a potential area to investigate in software compliance.

Similarly, other industries including financial, manufacturing, automobile, aviation, and government look at compliance concerns from an industry-specific perspective. The financial industry focuses on compliance issues related to transparency, accountability, and control. Manufacturing, automobile, and aviation industries have some similarities in compliance concerns, because they share relatively similar industry requirements. Specifically, safety standards and functional reliability are critical requirements for these industries. We also found that software compliance concerns are the least discussed by primary studies in the context of governments. Instead, their main focus is on interoperability aspects of e-Government services. Due to this and the fact that governments are highly complex systems, there is room for research on compliance concerns in governments. In general, all the frameworks discussed by primary studies

are industry-dependent and cannot fit into one another. This means that implementing the same software project in two different industries is more likely to experience different compliance issues, which are decided by the industry itself. Therefore, taking into account the industry-specific compliance needs when designing a software architecture is crucial to flexibility and adaptability of the software.

What all these frameworks share in common are the issues of changing requirements and policies, the gap between IT and laws, and the challenge of modeling policies and regulations in a way that can easily be reflected at the software level. However, based on compliance issues and frameworks discussed, we can classify industries into two groups. This classification is based on the level of details that the industries consider for their compliance requirements as well as the aspects that they look into. We classify software and cloud industries as one group, and all other industries as another group. Although there are some overlaps, the justification of this classification is that software and cloud industries tend to look at compliance concerns from the perspective of software development practices and service provisioning, while other industries look at the architectural level and from the industry-specific perspective. In other words, on the one hand, software and cloud industries discuss issues related to distributed teams, component licensing, SLA compliance, reliability, trust, service provisioning, and management. On the other hand, the other industries, including healthcare, manufacturing, finance, aviation and automobile, discuss software compliance at a higher level (i.e., compliance with industry standards, regulations, data sharing policies, and architectural perspective of software). Moreover, the proposed frameworks by primary studies are industry-dependent, emphasizing the importance of considering industry specific compliance requirements when designing a software architecture.

5 Conclusion

We used a systematic literature review, in order to survey existing frameworks and industry requirements regarding software compliance management. The review highlighted that many, different frameworks have been proposed for many industries to manage compliance of software and software services. There is no single solution that fits all scenarios and can be applied across all industries. Each industry has its own peculiarities, compliance requirements, and priorities, which need to be considered when managing software compliance accordingly. Nevertheless, there are common issues emphasized by many primary studies including the gap between compliance and software architecture, modeling policies and regulations, and enforcing those changes at a software level. Based on the analysis, there are two groups of industries that can be distinguished. The group composed of the software and cloud industries views compliance concerns from a component level, while the other group, which is composed of all other industries, looks at it from an architectural level. In other words, software and cloud industries focus on software compliance from a perspective of software development practices and service provisioning, while other industries focus on software compliance from a higher level perspective, which considers industry-

specific requirements and regulations. In future work, we will provide an extended study on tools and technologies used to manage and enforce software compliance.

As there is little research on software compliance in some industries (e.g., financial, government, automobile, and aviation), these industries and others are areas for future research. Furthermore, other potential directions for future research are: First, tools and technologies used for management and enforcement of software compliance; Second, technologies used for policy and legal modeling and the extent to which advances in technologies like AI and blockchain can help addressing it; Third, studies of software compliance in the context of government software projects with respect to compliance requirements and challenges.

References

1. Sefika M, Sane A, Campbell RH. Monitoring compliance of a software system with its high-level design models," in Proc of IEEE 18th Intl Conf on Software Engineering, Mar. 1996, pp. 387–396, doi: 10.1109/ICSE.1996.493433.
2. Singi K, RP JCB, Podder S, Burden AP. Trusted Software Supply Chain. In 34th IEEE/ACM Intl Conf on Automated Software Engineering (ASE), Nov. 2019, pp. 1212–1213, doi: 10.1109/ASE.2019.00141.
3. Harutyunyan N, Riehle D. Getting started with open source governance and compliance in companies. 2019, Accessed: Jan. 14, 2021. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/3306446.3340815.
4. Wurster M, Breitenbücher U, Falkenthal M, Leymann F. Developing, deploying, and operating twelve-factor applications with TOSCA. In Proc of 19th Intl Conf on Information Integration and Web-based Applications & Services, New York, NY, USA, Dec. 2017, pp. 519–525, doi: 10.1145/3151759.3151830.
5. González L. Ruggia R. Controlling Compliance of Collaborative Business Processes through an Integration Platform within an E-government Scenario. Jan. 2020, doi: 10.24251/HICSS.2020.245.
6. Zimmermann M, Breitenbucher U, Krieger C, Leymann F. Deployment Enforcement Rules for TOSCA-based Applications," Proc of Twelfth Intl Conf on Emerging Security Information, Systems and Technologies (SECURWARE 2018), pp. 114–121, 2018.
7. Lehman MM. Programs, life cycles, and laws of software evolution. Proc of IEEE, vol. 68, no. 9, Art. no. 9, Sep. 1980, doi: 10.1109/PROC.1980.11805.
8. Wettinger J, Behrendt M, Binz T, Breitenbücher U, Breiter G, Leymann F, Moser S, Schwertle I, Spatzier T. Integrating Configuration Management with Model-driven Cloud Management based on TOSCA. pp. 437–446, 2013.
9. Koetter F, Kochanowski M, Renner T, Fehling C, Leymann F. Unifying Compliance Management in Adaptive Environments through Variability Descriptors. In IEEE 6th Intl Conf on Service-Oriented Computing and Applications, Dec. 2013, pp. 214–219, doi: 10.1109/SOCA.2013.23.
10. Breitenbucher U, Binz T, Fehling C, Kopp O, Leymann F, Wieland M. Policy-Aware Provisioning and Management of Cloud Applications. International Journal On Advances in Security, vol. 7, p. 23, 2014.
11. Bostrom N. Superintelligence: Paths, Dangers. Strategies, Oxford University Press (2014).
12. Kitchenham BA, et al. Evidence-Based Software Engineering and Systematic Reviews. CRC Press, 2016.

13. Yun HY, Joe YJ, Shin DM. Method of license compliance of open source software governance. In: 8th IEEE Intl Conf on Software Engineering and Service Science (ICSESS). 2017. p. 83–6.
14. Singi K, Kaulgud V, Bose RPJC, Podder S. CAG: Compliance Adherence and Governance in Software Delivery Using Blockchain. In: IEEE/ACM 2nd Intl Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB). 2019. p. 32–9.
15. van der Burg S, Dolstra E, McIntosh S, Davies J, German DM, Hemel A. Tracing software build processes to uncover license compliance inconsistencies. In: Proc of 29th ACM/IEEE Intl Conf on Automated software engineering [Internet]. New York, NY, USA: ACM; 2014 [cited 2020 Oct 14]. p. 731–42. (ASE '14). Available from: https://doi.org/10.1145/2642937.2643013
16. McCarthy MA, Herger LM, Khan SM. A Compliance Aware Software Defined Infrastructure. In: IEEE Intl Conf on Services Computing. 2014. p. 560–7.
17. Suneel K, Guruprasad HS. A Novel Approach for SLA Compliance Monitoring in Cloud Computing. International Journal of Innovative Research in Advanced Engineering (IJIRAE). 2015 Jan 1;2(2).
18. Hashmi A, Ranjan A, Anand A. Security and Compliance Management in Cloud Computing. INTERNATIONAL JOURNAL OF ADVANCED STUDIES. 2018;7(1):8.
19. González L, Ruggia R. Controlling Compliance of Collaborative Business Processes through an Integration Platform within an E-government Scenario. In: Proc of 53rd Hawaii Intl Conf on System Sciences | 2020 [Internet]. 2020 [cited 2020 Oct 22]. Available from: http://scholarspace.manoa.hawaii.edu/handle/10125/63986
20. Gardazi SU, Ali A. Compliance-Driven Architecture for Healthcare Industry. International Journal of Advanced Computer Science and Applications. 2017 Jan 1;8.
21. Sartoli S, Ghanavati S, Siami Namin A. Compliance Requirements Checking in Variable Environments. In: IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC). 2020. p. 1093–4.
22. Li P, Xu C, Luo Y, Cao Y, Mathew J, Ma Y. CareNet: Building a Secure Software-defined Infrastructure for Home-based Healthcare. In: Proc of ACM Intl Workshop on Security in Software Defined Networks & Network Function Virtualization [Internet]. New York, NY, USA: ACM; 2017 [cited 2020 Oct 17]. p. 69–72. (SDN-NFVSec '17). Available from: https://doi.org/10.1145/3040992.3041007
23. Zimmermann M, Breitenbucher U, Krieger C, Leymann F. Deployment Enforcement Rules for TOSCA-based Applications. Proc of Twelfth Intl Conf on Emerging Security Information, Systems and Technologies (SECURWARE 2018). 2018;114–21.
24. Fischer MP, Breitenbucher U, Kepes K, Leymann F. Towards an Approach for Automatically Checking Compliance Rules in Deployment Models. Eleventh Intl Conf on Emerging Security Information, Systems and Technologies. 2017;5.
25. Tran H, Zdun U, Holmes T, Oberortner E, Mulo E, Dustdar S. Compliance in service-oriented architectures: A model-driven and view-based approach. Information and Software Technology. 2012 Jun 1;54(6):531–52.
26. Sharifi S, Parvizimosaed A, Amyot D, Logrippo L, Mylopoulos J. Symboleo: Towards a Specification Language for Legal Contracts. In: 2020 IEEE 28th Intl Requirements Engineering Conference (RE). 2020. p. 364–9.
27. Loreti D, Chesani F, Ciampolini A, Mello P. A distributed approach to compliance monitoring of business process event streams. Future Generation Computer Systems. 2018 May 1; 82:104–18.
28. Koetter F, Kochanowski M, Weisbecker A, Fehling C, Leymann F. Integrating Compliance Requirements across Business and IT. In: IEEE 18th Intl Enterprise Distributed Object Computing Conference. 2014. p. 218–25.

29. Groefsema H, van Beest N. Design-Time Compliance of Service Compositions in Dynamic Service Environments. In: IEEE 8th Intl Conf on Service-Oriented Computing and Applications (SOCA). 2015. p. 108–15.
30. Ingle C, Samudre A, Bhavsar P, Vidap PS. Audit and Compliance in Service Management using Blockchain. In: 2019 IEEE 16th India Council Intl Conf (INDICON). 2019. p. 1–4.
31. Hemel A, Kalleberg KT, Vermaas R, Dolstra E. Finding software license violations through binary code clone detection. In: Proc of the 8th Working Conf on Mining Software Repositories [Internet]. New York, NY, USA: ACM; 2011 [cited 2020 Oct 14]. p. 63–72. (MSR '11). Available from: https://doi.org/10.1145/1985441.1985453
32. German D, Di Penta M. A Method for Open Source License Compliance of Java Applications. IEEE Software. 2012 May;29(3):58–63.
33. Jeff H, Alan L. A Novel Method for Decentralised Peer-to-peer Software License Validation Using Cryptocurrency Blockchain Technology. In Australian Computer Society (ACS); 2015 [cited 2020 Oct 14]. Available from: https://openrepository.aut.ac.nz/handle/10292/10328
34. Koltun P. Free and Open Source Software Compliance: An Operational Perspective. IFOSS L Rev. 2011;3(1):95–102.
35. Von Willebrand M, Patanen M-P. Package Review as a Part of Free and Open Source Software Compliance. IFOSS L Rev. 2010. 2(1):39–60.
36. Brandic I, Dustdar S, Anstett T, Schumm D, Leymann F, Konrad R. Compliant Cloud Computing (C3): Architecture and Language Support for User-Driven Compliance Management in Clouds. In: IEEE 3rd Intl Conf on Cloud Computing. 2010. p. 244–51.
37. Foster H, Spanoudakis G, Mahbub K. Formal Certification and Compliance for Run-Time Service Environments. In: IEEE Ninth Intl Conf on Services Computing. 2012. p. 17–24.
38. Correia A, Brito e Abreu F. Defining and Observing the Compliance of Service Level Agreements: A Model Driven Approach. In: 2010 Seventh International Conference on the Quality of Information and Communications Technology. 2010. p. 165–70.
39. García-Galán J, Pasquale L, Grispos G, Nuseibeh B. Towards Adaptive Compliance. In: IEEE/ACM 11th Intl Symp on Software Engineering for Adaptive and Self-Managing Systems (SEAMS). 2016. p. 108–14.
40. Florian M, Paudel S, Tauber M. Trustworthy evidence gathering mechanism for multilayer cloud compliance. In: 8th Intl Conf for Internet Technology and Secured Transactions (ICITST-2013). 2013. p. 529–30.
41. Faniyi F, Bahsoon R. Self-managing SLA compliance in cloud architectures: a market-based approach. In: Proc of the 3rd Intl ACM SIGSOFT Symp on Architecting Critical Systems [Internet]. New York, NY, USA: ACM; 2012 [cited 2020 Oct 14]. p. 61–70. (ISARCS '12). Available from: https://doi.org/10.1145/2304656.2304665
42. Subramaniam C, Natarajan K. Software Reliability Compliance Model for Requirements Faults. In: In Recent Trends in Communications and Computers. Proc of 16th WSEAS Intl Conf on Communications. 2012. p. 332–40.
43. Castellanos Ardila JP, Gallina B. Separation of Concerns in Process Compliance Checking: Divide-and-Conquer. In Springer International Publishing; 2020 [cited 2020 Oct 15]. Available from: http://urn.kb.se/resolve?urn=urn:nbn:se:mdh:diva-49334
44. Singh S, Sidhu J. Compliance-based Multi-dimensional Trust Evaluation System for determining trustworthiness of Cloud Service Providers. Future Generation Computer Systems. 2017 Feb 1; 67:109–32.
45. Krieger C, Breitenbücher U, Képes K, Leymann F. An Approach to Automatically Check the Compliance of Declarative Deployment Models. In: IBM Research Division. 2018. p. 76–89.
46. Carrasco J, Cubo J, Durán F, Pimentel E. Bidimensional Cross-Cloud Management with TOSCA and Brooklyn. In: IEEE 9th Intl Conf on Cloud Computing. 2016. p. 951–5.

47. Qanbari S, Sebto V, Dustdar S. Cloud Resources-Events-Agents Model: Towards TOSCA-Based Applications. In: Villari M, Zimmermann W, Lau K-K, editors. Service-Oriented and Cloud Computing. Berlin, Heidelberg: Springer; 2014. p. 160–70.
48. Koetter F, Kochanowski M, Renner T, Fehling C, Leymann F. Unifying Compliance Management in Adaptive Environments through Variability Descriptors (Short Paper). In: IEEE 6th Intl Conf on Service-Oriented Computing and Applications. 2013. p. 214–9.
49. R P JCB, Singi K, Kaulgud V, Phokela KK, Podder S. Framework for Trustworthy Software Development. In: 34th IEEE/ACM Intl Conf on Automated Software Engineering Workshop (ASEW). 2019. p. 45–8.
50. Breitenbucher U, Binz T, Fehling C, Kopp O, Leymann F, Wieland M. Policy-Aware Provisioning and Management of Cloud Applications. International Journal on Advances in Security. 2014; 7:23.
51. Ingolfo S, Siena A, Mylopoulos J, Susi A, Perini A. Arguing regulatory compliance of software requirements. Data & Knowledge Engineering. 2013 Sep 1; 87:279–96.
52. Thalmann S, Bachlechner D, Demetz L, Manhart M. Complexity is dead, long live complexity! How software can help service providers manage security and compliance. Computers & Security. 2014 Sep 1; 45:172–85.
53. Gangadharan GR, D'Andrea V, De Paoli S, Weiss M. Managing license compliance in free and open source software development. Inf Syst Front. 2012 Apr 1;14(2):143–54.
54. Khan KM, Yun Bai. Automatic verification of health regulatory compliance in cloud computing. In: IEEE 15th Intl Conf on e-Health Networking, Applications and Services (Healthcom 2013). 2013. p. 719–21.
55. Hamou-Lhadj A. Regulatory compliance and its impact on software development. Software Compliance Research Group, Department of Electrical and Computer Engineering. 2015.
56. Truong N-T, Nguyen V-H. An approach to checking the compliance of user permission policy in software development. Int J Soft Eng Knowl Eng. 2013 Oct 1;23(08):1139–51.
57. Elhasnaoui S, Drissi S, Iguer H, Medromi H. Multi-Agent Architecture of Intelligent and Distributed Platform of Governance, Risk and Compliance of Information Systems. IJACSA [Internet]. 2019 [cited 2020 Dec 17];10(5). Available from: http://thesai.org/Publications/ViewPaper?Volume=10&Issue=5&Code=IJACSA&SerialNo=10
58. Jensen M, Kapila S, Gruschka N. Towards Aligning GDPR Compliance with Software Development: A Research Agenda. 2019. 389 p.
59. Marques J, Cunha AM da. 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). 2018. p. 1–8.
60. Kittmann T, Lambrecht J, Horn C. A privacy-aware distributed software architecture for automation services in compliance with GDPR. In: 2018 IEEE 23rd Intl Conf on Emerging Technologies and Factory Automation (ETFA). 2018. p. 1067–70.
61. Moyon F, Beckers K, Klepper S, Lachberger P, Bruegge B. Towards Continuous Security Compliance in Agile Software Development at Scale. In: 2018 IEEE/ACM 4th Intl Workshop on Rapid Continuous Software Engineering (RCoSE). 2018. p. 31–4.
62. Arogundade OT, Abioye TE, Mustapha AM, Adeniji AM, Ikotun AM, Asahiah FO. Specifying and Incorporating Compliance Requirements into Software Development Using UML and OCL. In: Gervasi O, Murgante B, Misra S, Stankova E, Torre CM, Rocha AMAC, ed. Computational Science and Its Applications (ICCSA). Springer. 2018. p. 511–26.
63. Engiel P, Leite JCSDP, Mylopoulos J. A tool-supported compliance process for software systems. In: 11th Intl Conf on Research Challenges in Information Science (RCIS). 2017. p. 66–76.
64. Lepmets M, McBride T, McCaffery F. Towards Safer Medical Device Software Systems: Industry-Wide Learning from Failures and the Use of Safety-Cases to Support Process

Compliance. In: 10th Intl Conf on the Quality of Information and Communications Technology (QUATIC). 2016. p. 193–8.
65. Savarimuthu T, Dam H, Licorish S, Keertipati S, Avery D, Ghose A. Process Compliance in Open Source Software Development – A Study of Python Enhancement Proposals (PEPS). Research Papers [Internet]. 2016 Jun 15; Available from: https://aisel.aisnet.org/ecis2016_rp/48
66. Chakraborty M, Chaki N. A New Framework for Configuration Management and Compliance Checking for Component-Based Software Development. In: Chaki R, Cortesi A, Saeed K, Chaki N, editors. Advanced Computing and Systems for Security: Vol 2 [Internet]. New Delhi: Springer India; 2016 [cited 2020 Dec 18]. p. 173–88. (Advances in Intelligent Systems and Computing). Available from: https://doi.org/10.1007/978-81-322-2653-6_12
67. Jorshari FZ, Tawil RH. A High-Level Scheme for an Ontology-Based Compliance Framework in Software Development. In: IEEE 17th Intl Conf on High Performance Computing and Communications, IEEE 7th Intl Symp on Cyberspace Safety and Security, and IEEE 12th Intl Conf on Embedded Software and Systems. 2015. p. 1479–87.
68. Zema M, Rosati S, Gioia V, Knaflitz M, Balestra G. Developing medical device software in compliance with regulations. In: 2015 37th Annual Intl Conf of the IEEE Engineering in Medicine and Biology Society (EMBC). 2015. p. 1331–4.
69. Hocking AB, Knight J, Aiello MA, Shiraishi S. Arguing Software Compliance with ISO 26262. In: IEEE Intl Symp on Software Reliability Engineering Workshops. 2014. p. 226–31.
70. Vytautas Č, Friedrich L. Compliance and Software Transparency for the Design of Legal Machines. In 2014.
71. Jurnečka P, Hanáček P, Barabas M, Henzl M, Kačic M. A method for parallel software refactoring for safety standards compliance. In: 8th IET Intl System Safety Conference incorporating the Cyber Security Conference 2013. 2013. p. 1–6.
72. Ozbas-Caglayan K, Dogru AH. Software Repository Analysis for Investigating Design-Code Compliance. In: Joint Conf. of 23rd Intl Workshop on Software Measurement and 8th Intl Conf on Software Process and Product Measurement. 2013. p. 231–4.
73. Magnusson C, Chou S. Risk and Compliance Management Framework for Outsourced Global Software Development. In: 5th IEEE Intl Conf on Global Software Engineering. 2010. p. 228–33.
74. Maxwell JC, Antón AI. The production rule framework: developing a canonical set of software requirements for compliance with law. In: Proc of 1st ACM Intl Health Informatics Symp [Internet]. New York, NY, USA: ACM; 2010 [cited 2020 Dec 18]. p. 629–636. (IHI '10). Available from: https://doi.org/10.1145/1882992.1883092
75. Kim K, Altmann J. Platform Provider Roles in Innovation in Software Service Ecosystems. IEEE Transactions on Engineering Management, https://doi.org/10.1109/TEM.2019.2949023, 2020.
76. Haile N, Altmann J. Evaluating Investments in Portability and Interoperability between Software Service Platforms. Future Generation Computer Systems 78(1): 224-241, https://doi.org/10.1016/j.future.2017.04.040, Elsevier, January 2018.
77. Breskovic I, Altmann J, Brandic I. Creating Standardized Products for Electronic Markets," Future Generation Computer Systems, Elsevier, 29(4): 1000-1011, June 2013.

Reviewing the Interrelation Between Information Security and Culture: Toward an Agenda for Future Research

Sebastian Hengstler[1], Natalya Pryazhnykova[1]

[1] Chair of Information Security and Compliance, University of Goettingen, Germany
s.hengstler@stud.uni-goettingen.de, pryazhnykova@gmail.com

Abstract. The main goal of this paper is to provide a review of existing research on the interrelationships between information security and culture. The results of this study are based on a structured literature review of current research on the interrelationships between information security and culture, published between 2000 and 2020 (September). Our results show that current research has focused on four core themes: (1) the influence of culture on information security policy compliance behavior, (2) information security culture in organizations, (3) the influence of culture on information security awareness programs and (4) the effect of culture on information security governance. Our results show, that so far, the mentioned topics have been investigated from different perspectives. However, our results offer potential for future research, e.g. in the connections between information security and individual cultural values or in the area of information security awareness.

Keywords: Information Security and Culture, Literature Review, Information Security

1 Introduction

Information security represents a field of increasing scholarly interest from a practical and theoretical perspective and includes various critical dimensions, which need to be considered to ensure a high level of information security e.g. in organizations [1]. Important mechanisms to guarantee information security are technical measures, such as firewalls, to protect networks or various authorization measures for hardware protection [2].

However, it is a well-known fact that attacks on information security systems in private or professional usage start at the weakest point which is failure caused by an individual [3]. This is the reason, why measures to ensure compliant behavior of employees in various organizations are becoming increasingly crucial [4].

Existing studies analyze a variety of mechanisms that influence the compliance behavior of employees, such as the social environment of an individual, the use of informal and formal sanctions to ensure compliance or the use of threat and coping

16th International Conference on Wirtschaftsinformatik,
March 2021, Essen, Germany

appraisals [1]. Furthermore, existing research presents, that contextual differences are an essential factor to consider, when designing information security measures to achieve compliance behavior [5]. Besides the distinction between different types of information security breaches, culture is an important contextual component of current information security research [6].

Over the last two decades, culture has been analyzed from different angles in the context of information security and there are different approaches in research, which aim to explain how these two aspects relate. The results of existing literature reviews in the field of information security and culture show a variety of different outcomes. Mahfuth et al. (2017) analyzed existing research regarding information security, organizational culture and the relation of these two fields. [7]. Karlsson and Åström (2015) provide an overview of the research in the area of information security culture [6]. Hina and Dominic (2020) identify information security and culture as current trending topic in information security research [8]. In summary, there are recent approaches, which analyze the interrelations between information security and culture from different perspectives. However, we believe that a comprehensive overview that represents the different perspectives and top themes of information security culture research is still missing, but can help to provide a more complete view on the relation of culture and information security [9].

The aim of this paper is to summarize existing research about information security and culture in order to increase the understanding of the influence of culture and its relevance to information security. The scope of this paper is to identify the current research themes in this field, and to provide further directions for future research. In our analysis, we build on existing cultural concepts to identify interrelations between culture and information security research. We used the approach of Leidner and Kayworth (2006) to analyze the interrelations between culture and information security, in combination with the process for a structured literature analysis of Webster and Watson (2002) [9, 10].

With our research, we aim to contribute to current literature in providing a comprehensive view on the current state of the interrelation between information security and culture research. Our study provides an overview not only about analyzed cultural levels and artefacts, but also used research approaches (methods and theories). In addition to that, we identified overlapping and less analyzed aspects in existing research. We identified both major and minor gaps in the literature and provided implications for further research.

This study is structured as follows. In section 2, we defined the relevant concepts of culture we used in our literature analysis. In section 3, the literature analysis process is explained. We described outcomes of this paper and defined focus themes in information security and culture research in section 4. An overview about potential future research is presented in section 5. The paper concludes in section 6.

2 The Concept of Culture

In other research areas such as Social Studies or Psychology, culture is understood as a summary of ideologies, beliefs, basic assumptions, shared norms and values, that have an influence on the collective will [11, 12]. Other approaches analyze the construct of culture from a different perspective and focus on individual cultural dimensions, which describe the individual components of culture [13]. Schein's (1997) three-level model of culture shows a model to explain culture within organizations [14]. Due to these differences and the fact, that the concept of culture is characterized by its many meanings and possible interpretations, it is rather challenging to define an overall definition of the concept of culture [15]. The first modern interpretation was made by Edward Tylor, who described culture as the collection of all skills and habits such as knowledge, beliefs or laws, which are shaped by society [16]. Hofstede specified the shaping of behavior by society and defined culture as a collective coding of the mind by which the members of a group distinguish themselves from the members of other groups [12]. Because of the fact that culture includes all rules, norms and the code of conduct of a collective, it has an influence on the behavior of the individuals of a group and is consequently controlling behavior [17].

In the area of information systems, the extent to which these are related to the topic of culture was also investigated. Leidner and Kayworth (2006), for example, analyzed different approaches in the area of information systems and culture in terms of their underlying theoretical cultural artifacts. They pointed out, that a relation between information systems and these cultural artefacts can occur on several levels of culture. Examples of this are a connection in the context of IT culture, the IT adoption process and cultural dependencies in IT management. In their analysis they distinguish between the national, organizational, and individual levels of analysis and name several cultural artefacts, which are used in research to analyze the interrelation between culture and information systems [9]. The national unit of analysis is described as the analysis of cultural orientation, based on a samples nationality, where different countries are chosen as the object of the study [12]. At the organizational level, studies analyze cultural differences in different organizational units, e.g. in different companies [14]. The analysis of smaller groups or individuals describes the study of individual behavior or within social groups [18]. As a subdiscipline of information systems research, we can relate these findings to current topics in information security research [6, 7]. For example, topics such as security culture, compliance behavior or security management can also be identified in the security domain, which show similarities to existing information systems research in other research streams. To make the results of our analysis comparable to existing research, we adapt Leidner and Kayworth's (2006) approach and analyze the identified literature, based on used cultural artifacts and their level of analysis [9].

3 Literature Analysis Process

For the literature analysis we adapt the methodological approach established in the field of information systems research according to Webster and Watson (2002) [10], which provides a solution for the systematic identification and analysis of relevant literature. The following plan was used for the consistent implementation of the methodological approach in our literature analysis. Firstly, the subject area was defined and our target group for our research was specified. At this point, our intention was to determine the current state of the research about the influence of culture on information security. Therefore, we concentrated on research outcomes, that shed light on the connection between these two topics. The scope of our literature review is to identify central topics in the interrelation of these research areas. We address mainly specialized scholars analyzing the effect of culture on information security or scholars interested in cross-cultural research in the field of information security.

Secondly, we conceptualized the core elements that will be used for the systematic categorization of identified literature. In order to classify and analyze the identified literature with respect to our research purpose, we have transferred the common characteristics of this research area from existing literature reviews, namely the methodological approach, cultural level of analysis, underlying theories and considered cultural artefacts, and used them in the form of a concept matrix for the analysis of our identified literature [9, 12, 13].Thirdly, we specified characteristics, which we wanted to analyze, the databases selection and the definition of our search terms.

Since research in the field of information security and culture is published in conference proceedings as well as in international journals, we used different databases. The databases EbscoHost, Aisel and AbiInform were used to obtain a broad coverage of both international journals and conference proceedings in our research area. Forward and backward search was conducted with the database Web-of-Science. Generally, publications in relevant journals and conferences of information security research were considered in our analysis. Publications from other disciplines in our research area were also included if they were of high relevance (e.g. high citation rate). We followed the orientation of Karlsson and Åström (2015) and considered literature published since 2000 [6]. In order to identify potentially relevant literature, we analyzed the keywords, the abstract and the title of the respective studies. The use of the search queries in the different databases resulted in a list of 461 publications, including duplicates. After deleting duplicates and articles with incorrect content that were not in the focus of our analysis, we received a list of 103 articles to be analyzed. 53 of these articles were identified in the initial search, 37 in the forward search and 13 in the backward search. In total, 58 articles where published in information systems or computer science journals and 45 articles on related conferences. A list of our search terms and constructs used to classify the results is shown in Table 1.

Table 1. Search terms and analyzed concepts.

Search Terms	Analyzed Concepts
Information security culture	Theories
Information security AND culture	Cultural Dimensions
Information security AND organizational culture	Used Methodical Approach
Information security AND national culture	Cultural Level of Analysis (National, Organizational, Individual/Subunit)
Information security AND information security culture	

In a fourth step, we analyzed the identified literature according to the identified characteristics. We considered articles published between 2000 and 2020 (September). An Overview about the considered articles per journal/conference is shown in table 2.

Table 2. Identified articles by journal and conference

Journal Title	Amount
Organizational behavior Computers & Security	1
Information Systems Management	2
Information Management & Computer Security	9
Computers in Human Behavior	2
Information & Management	2
Computers & Security	15
Information and Computer Security	6
Information Systems Journal	2
Communications of the Association for Information Systems	2
Southern African Business Review	1
Computer Fraud Security	2
Journal of Theoretical and Applied Information Technology	1
South African Computer Journal	1
Journal of Enterprise Information Management	1
Electronic Markets	1
Journal of Global Information Management	1
Decision Sciences	1
MIS Quarterly	2
Journal of Computer Information Systems	1
Journal of Database Management	1
Information Technology and Management	1
Journal of Global Information Technology Management	1

Conference Title	Amount
International Conference on Research and Innovation in Information Systems (ICRIIS)	1
Pacific Asia Conference on Information Systems (PACIS)	5
American Conference on Information Systems (AMCIS)	6
European Conference on Information Systems (ECIS)	4
International Conference on Information Systems (ICIS)	1
Human Aspects of Information Security & Assurance (HAISA)	2
International Social Security Association (ISSA)	3
International Conference on Information Security and Cryptology (ICISC)	3
IEEE World Congress On Computer Applications and Information Systems (WCCAIS)	1
Australian Information Security Management Conference (AISM)	6
International Carnahan Conference on Security Technology (ICCST)	1
Conference on Information Security for South Africa (ISSA)	1
Hawaii International Conference on System Sciences (HICSS)	1
Wireless Internet Service Providers Conference (WISP)	4
International Information Management Association Conference (IIMA)	1
Mediterranean Conference on Information Systems (MCIS)	1
International Conference for Internet Technology and Secured Transactions (ICITS)	1
Workshop on Governance of Technology, Information and Policies	1
European Conference on Information Warfare and Security (ECIW)	1
International Conference on Availability, Reliability and Security	1

Finally, the identified topics of existing literature were discussed, and current trends and further research potential were presented. We describe the last two steps in the following chapters.

4 Results

A total of 103 articles were analyzed in this literature review. Among them, 28 articles examined culture at the national level in the context of information security and 63 examined culture at the organizational level. There were 8 studies that examined culture at the individual/subunit level in the context of information security. Over 71% of the studies on the national cultural level used Hofstede's culture dimensions [12]. The organizational level studies often do not use explicit cultural artifacts (68%). The most represented cultural artifact at the organizational level is Schein's (1992) model of organizational culture (12%) [14]. No explicit cultural artifacts were studied on the individual/subunit cultural level. Additionally, we categorized the articles by their

scientific approach. Overall, there are two trends which were identified for the methodological approaches. 23% of the articles rely on conceptual frameworks. 32% of the identified articles used a questionnaire-based, quantitative methodological approach. Other methodological approaches are less represented. In terms of used theories, many articles have a more theory generating nature and do not use an existing theory (66%) for their studies. The types of theories do not indicate a focus.

Furthermore, we were able to identify overall focus themes within the analyzed articles dealing with the interrelations between information security and culture: (1) the influence of culture on information security policy compliance behavior, (2) information security culture in organizations, (3) the influence of culture on information security awareness programs and (4) the effect of culture on information security governance. We were not able to assign three identified articles to the mentioned articles and did not consider them in more detail. The following chapters describe the identified focus topics in more detail. A list of the identified and characterized literature, based on our observed concepts of theories, methods, cultural artifacts, and cultural level of analysis is listed in the appendix (Tables 4-7).

4.1 The Influence of Culture on Information Security Policy Compliance Behavior

A total of 30 papers dealt with the influence of culture on information security policy compliance behavior. 18 of these studies focused on the national cultural level, 11 on the organizational cultural level, and one on the individual/subunit cultural level. The majority of the articles used a questionnaire-based, quantitative approach (18), whereas 7 articles chose a qualitative approach. Meta-analyses (1), commentaries (2) typologies (1), case studies (2), and mixed method approaches (1) are less represented. Most articles do not explicit use a theory and are more theory generating in nature (11). The most frequently used theories are the theory of planned behavior (3) and the deterrence theory (4). Other theories are represented sporadically. At the national cultural level, 13 of 18 articles used Hofstede's cultural dimensions as cultural artifacts [12]. At the organizational level, hardly any culture artifacts have been used.

The topic “influence of culture on information security policy compliance behavior includes articles that primarily focus on the analysis of cultural differences regarding information security compliance behavior of employees. There is only one study, which considers individual cultural values when analyzing information security compliance behavior with respect to cultural differences. On a national cultural level, the research focus lies in the analysis of the effectiveness of different theoretical mechanisms on compliance behavior along national cultures. In this area, different theories such as deterrence theory or the theory of planned behavior are analyzed [19–21]. The focus is mainly on the analysis of 7 different cultures and does not show a big variety [22]. On the organizational culture level, research in this topic area focuses on organizational concepts that positively influence information security behavior and thereby contribute to a positive security culture in organizations. For example, knowledge sharing [23], discipline and agility [24], and morale within an organization are examined in terms of their positive impact on behavior [25].

4.2 Information Security Culture in Organizations

A total amount of 39 papers have dealt with information security culture in organizations. 32 studies focused on the organizational cultural level, 6 on the individual/subunit cultural level, and one study on a national cultural level. Predominantly, conceptual frameworks were developed within the articles (14). There is also a focus on conducting literature reviews (5), qualitative studies and case studies (5), and questionnaire-based quantitative studies (7). Most articles do not use explicit theory and are more theory generating in nature (34). At the organizational cultural level, Schein's (1992) organizational behavior theory was frequently used (7) [14]. Most articles do not mention explicitly cultural artifacts (26).

The theme "information security culture in organizations" includes articles, focusing on concepts and influencing factors of an information security culture within organizations, namely conceptualization of cultural models, their validation and the analysis of factors influencing a security culture and their effects. At the individual or subunit level, the crucial point lies in identifying different cultural subgroups within an organization, e.g. through different professional backgrounds [26, 27]. Another aspect of an information security culture is the analysis of influencing factors on such cultural subgroups [28, 29]. On an organizational cultural level, some articles focus on the analysis of illusory concepts of an organizational culture and their application in the information security culture domain [30–32]. Another core issue is the analysis of factors that influence an information security culture [33–35]. Furthermore, similarities between the traditional view of organizational cultures and an information security culture are in focus of current research as well [36, 37]. Other articles concentrate on the managerial impact on information security culture, such as the role of CISO's [38] or managerial guidelines to lead in a security culture [31].

4.3 The Influence of Culture on Information Security Awareness Programs

The influence of culture on information security awareness (ISA) programs was covered by a total of 8 articles. There were two studies with a focus on organizational cultural level, one study on the individual/subunit cultural level and five studies on national cultural level. Predominantly, mostly questionnaire-based, quantitative studies were carried out (5). Two articles conducted an experiment for their study and one article used a qualitative approach. A total of four studies chose Hofstede's culture dimensions as culture artifacts [12]. Other cultural artifacts, such as the organizational behavior theory [14] and aspects from the competing value framework were used as well [39]. In the context of this topic, different ways of approaching information security and culture were identified. On the one hand, correlations between information security awareness measures and the security culture of an organization are analyzed. The authors show that the security culture can have an influence on the individual awareness behavior of employees [40]. On the other hand, there are studies which investigate the influence of different organizational factors on ISA from different cultural perspectives. This includes the analysis of the impact of factors, such as

security culture or competing values on the awareness of employees [41]. At the national cultural level, studies have been mainly conducted with the purpose to analyze the effectiveness of theoretical mechanisms, such as social norms and attitude values [41] or fear appeals [42] on information security awareness in different countries.

4.4 The Effect of Culture on Information Security Governance

The effect of culture on information security governance was analyzed by a total of 21 articles. There were 17 studies with a focus on organizational cultural level and 4 studies on national cultural level. Most of the analyzed studies focused on qualitative research approaches (5) and case studies (6). Most articles did not explicit outline mentioned theoretical approach or specific used cultural artefacts.
National cultural level studies in this theme focus on analyzing national cultural values on the effectiveness of security measures [43] and what national-level factors need to be considered while implementing them [44]. Other studies at the national level analyze the influence of national culture on corporate structure [45] and information security risk management [46]. At the organizational level of analysis, several focus themes can be identified.

On the one hand, current research is concerned with the relationship between culture and information security management. This includes the analysis of what effect management behavior can have on information security and its culture in the organization [47, 48] and the influence of culture on information security management itself [49]. Another element is the description of governance structures and their constituents for information security, considering cultural factors. This consists of the influence of culture on organizational structures, the implementation of information security measures [50] and the differences within these structures in different organizations [51]. Closely related are articles dealing with the design of information security policies, predominantly with the consideration of cultural differences [8, 52]. Another subtopic regarding the effect of culture on information security governance are Assessments. Articles describe not only the design and validation of assessment tools for information security culture, but also the implementation of monitoring methods for information security in a cross-cultural context [53, 54].

5 Directions for Future Research

Our study examined the current focus of analyses regarding the interrelation of culture and information security. In our literature review, we identified 103 relevant articles and were able to identify four focus themes concerning the interrelation between culture and information security. According to the outcomes of this study, the potential for further research can be identified.

Within the topic “the influence of culture on information security policy compliance behavior” there is a strong focus regarding the national cultural level of analysis and the testing of the effectiveness of various theories in respect of different national cultures. The focus lies mainly in theories established in security research, such as

deterrence theory or the theory of planned behavior. Additionally, the individual characteristics of the culture of individual employees have not yet been taken into account. Future research in the field of the relation of culture and information security behavior should include: (1) The investigation of further theoretical mechanisms and their cultural dependency regarding information security behavior, such as theories explaining the shaping process of behavior by social factors [6]. (2) A focus on the influence of individual manifestations of cultural artifacts on behavior, in order not to make assumptions about dependencies between culture and individual behavior based on only national cultural values [55].

The topic of information security culture in organizations includes articles about the structure of a security culture within organizations and its influencing factors. Research in this area could benefit from an increased use of established organizational culture theories or culture artifacts not only to validate the already developed information security culture frameworks but also to draw parallels to organizational culture [35]. Furthermore, previous studies have predominantly focused on looking at the whole organization and its security culture. Differences in individual sub-units, such as different professions or demographic or geographic factors are poorly represented The focus of future research in this area should therefore provide: (1) A validation of the previously developed frameworks in the security culture environment, taking into account established cultural artifacts in the organizational culture domain. (2) A more specific investigation of security culture in different sub-units of organizations and their factors influencing each other [26].

The theme about the influence of culture on information security awareness programs has been poorly established in current research, with only 8 articles published Overall, it is visible that the relationships between cultural artifacts and ISA have been lack of analysis. On a national cultural level, it is evident, that culture has an influence on ISA. Rather a few studies exist in connection with organizational factors, culture and ISA, as well as the influence of individual cultural values on ISA. Accordingly, our proposal for future research in this area broadly determined. We suggest that future research on the relationship between culture and ISA should focus on: (1) The interrelationships of culture at the national, organizational, and individual/subunit levels with ISA, taking into account established ISA approaches, in order to provide more insights into the interrelationships of these two aspects [40].

Articles examining the effect of culture on information security governance are characterized by the study of factors influencing culture on governance structures or structures of the organization itself. Likewise, a relatively large number of articles on the influence of culture on information security management can be identified. What has been less considered so far is the conceptualization and review of methods and tools for reviewing security measures under consideration of cultural differences in order to build an international, cross-cultural monitoring of the effectiveness of security measures [50]. Consequently, we suggest that future research focus on the relationship between cultural artifacts and the conceptualization and review of assessment and monitoring approaches. Our results are summarized in table 3.

Table 3**.** Research agenda.

Theme	We need to…	Limitations to Overcome
The Influence of Culture on Information Security Policy Compliance Behavior	(1) Further investigate theoretical mechanisms and their cultural dependency regarding information security behavior. (2) Analyze the influence of individual cultural values on behavior.	(1) A focus on quantitative studies (2) The consideration of cultural artefacts in studies about information security behavior and their relation to culture
Information Security Culture in Organizations	(1) Validate previously developed frameworks in the security culture environment, taking into account established cultural artifacts. (2) Investigate security culture in different sub-units of organizations and their factors influencing each other.	(1) Limitations of conceptual Frameworks (2) The distinction between different types of organizations
The Influence of Culture on Information Security Awareness Programs	(1) Analyze the interrelationships of culture at the national, organizational, and individual/subunit levels (2) Go beyond quantitative approaches and use a greater variety of qualitative and quantitative approaches.	(1) A focus on national cultural values (2) A focus on quantitative studies
The Effect of Culture on Information Security Governance	(1) Further analyze the relationship between cultural artifacts and the conceptualization and review of assessment and monitoring approaches. (2) Measure culture not only on organizational, but individual level to better understand the individual effect of culture on governance structures.	(1) The lack of theoretical approaches in this research stream (2) A focus on national cultural values

6 Conclusion

The purpose of this study was to analyze current research on the relationships between information security and culture. Our study focuses on the interrelationships between information security and culture and thus represents an extension to existing literature reviews in the security context. By applying a structural framework, it provides an overview of the current state of research and its core topics, as well as existing research gaps. Based on the literature we identified, we were able to identify open points in the identified core topics and highlight potential for future research. Overall, limitations

remain to be identified in the context of our study. Our findings are limited to the selected areas of outlets and keywords that we considered in our search for relevant literature. Future research in specific research areas, will need to be further elaborated to include a wider scope of other, IS conferences, and journals potentially relevant to the specific case.

References

1. Moody, G.D., Siponen, M., Pahnila, S.: Toward a Unified Model of Information Security Policy Compliance. MIS Quarterly 42, 285–311 (2018)
2. D'Arcy, J., Hovav, A.: Does One Size Fit All? Examining the Differential Effects of IS Security Countermeasures. Journal of Business Ethics 89, 59–71 (2009)
3. Siponen, M., Vance, A.: Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. MIS Quarterly 34, 487 (2010)
4. Puhakainen, P., Siponen, M.: Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. MIS Quarterly 34, 757 (2010)
5. Aurigemma, S., Mattson, T.: Generally Speaking, Context Matters: Making the Case for a Change from Universal to Particular ISP Research. Journal of the Association for Information Systems (2019)
6. Karlsson, F., Åström, J., Karlsson, M.: Information security culture – state-of-the-art review between 2000 and 2013. Info and Computer Security 23, 246–285 (2015)
7. Mahfuth, A., Yussof, S., Baker, A.A., Ali, N.'a.: A systematic literature review: Information security culture. In: Social transformation through data science. ICRIIS 2017 : 5th International Conference on Research and Innovation in Information Systems : Adya Hotel, Langkawi, Kedah, 16-17th July 2017, pp. 1–6. IEEE, Piscataway, NJ (2017)
8. Hina, S., Dominic, P.D.D.: Information security policies' compliance: a perspective for higher education institutions. Journal of Computer Information Systems 60, 201–211 (2020)
9. Leidner, D.F., Kayworth, T.: Review: a review of culture in information systems research: toward a theory of information technology culture conflict. MIS Quarterly 30 (2006)
10. Jane Webster, Richard T. Watson: Analyzing the Past to Prepare for the Future: Writing a Literature Review. MIS Quarterly 26 (2002)
11. Straub, D., Loch, K., Evaristo, R., Karahanna, E., Srite, M.: Toward a Theory-Based Measurement of Culture. Journal of Global Information Management 10, 13–23 (2002)
12. Hofstede, G.: Culture's consequences. Comparing values, behaviors, institutions, and organizations across nations. Sage Publ, Thousand Oaks, Calif. (2011)
13. Nonaka, I.: A Dynamic Theory of Organizational Knowledge Creation. Organization Science 5, 14–37 (1994)
14. Schein, E.H.: Organizational culture and leadership. Jossey-Bass, San Francisco (1997)
15. Sabel, N., Rietz, S.: Interkulturelle Kompetenz: Einfluss der Kultur auf das internationale Management. Einfluss der Kultur auf das internationale Management. Diplomica Verlag GmbH, Hamburg (2010)
16. Tylor, E.B.: Primitive culture. Researches into the development of mythology, philosophy, religion, art, and custom. Cambridge Univ. Press, Cambridge (2010)

17. Keller, E. von: Die kulturvergleichende Managementforschung. Gegenstand, Ziele, Methoden, Ergebnisse und Erkenntnisprobleme einer Forschungsrichtung. Haupt, Bern (1982)
18. Karahanna, E., Evaristo, J.R., Srite, M.: Levels of Culture and Individual Behavior. Journal of Global Information Management 13, 1–20 (2005)
19. Dinev, T., Goo, J., Hu, Q., Nam, K.: User behaviour towards protective information technologies: the role of national cultural differences. Info Systems J 19, 391–412 (2009)
20. Hovav, A., D'Arcy, J.: Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. Information & Management 49, 99–110 (2012)
21. Hovav, A., D'Arcy, J., Lee, K.: A Cross-Cultural Analysis of Security Countermeasure Effectiveness. In: WISP 2007 (2007)
22. Cram, W.A., D'Arcy, J., Proudfoot, J.G.: Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance. MISQ 43, 525–554 (2019)
23. Rocha Flores, W., Antonsen, E., Ekstedt, M.: Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. Computers & Security 43, 90–110 (2014)
24. AlKalbani, A., Deng, H., Kam, B.: Organisational Security Culture and Information Security Compliance for E-Government Development: The Moderating Effect of Social Pressure. In: PACIS, p. 65 (2015)
25. Amankwa, E., Loock, M., Kritzinger, E.: Establishing information security policy compliance culture in organizations. Info and Computer Security 26, 420–436 (2018)
26. Ramachandran, S., Rao, C., Goles, T., Dhillon, G.: Variations in Information Security Cultures across Professions: A Qualitative Study. CAIS 33 (2013)
27. Ramachandran, S., Rao, S.V., Goles, T.: Information Security Cultures of Four Professions: A Comparative Study. In: Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008), p. 454. IEEE (2008 - 2008)
28. van Niekerk, J., Solms, R. von: A holistic framework for the fostering of an information security sub-culture in organizations. In: Issa, 1 (2005)
29. da Veiga, A., Martins, N.: Defining and identifying dominant information security cultures and subcultures. Computers & Security 70, 72–94 (2017)
30. Nel, F., Drevin, L.: Key elements of an information security culture in organisations. Info and Computer Security 27, 146–164 (2019)
31. van Niekerk, J.F., Solms, R. von: Information security culture: A management perspective. Computers & Security 29, 476–486 (2010)
32. Williams, P.A.: What Does Security Culture Look Like For Small Organizations? Security Research Institute (SRI), Edith Cowan University (2009)
33. Al Natheer, M., Chan, T., Nelson, K.: Understanding and measuring information security culture (2012)
34. Dojkovski, S., Lichtenstein, S., Warren, M.J.: Fostering information security culture in small and medium size enterprises: an interpretive study in Australia (2007)
35. Dhillon, G., Syed, R., Pedron, C.: Interpreting information security culture: An organizational transformation case study. Computers & Security 56, 63–69 (2016)
36. Ruighaver, A.B., Maynard, S.B., Chang, S.: Organisational security culture: Extending the end-user perspective. Computers & Security 26, 56–62 (2007)

37. Ruighaver, A.B., Maynard, S.B.: Organizational Security Culture: More Than Just an End-User Phenomenon. In: Fischer-Hübner, S., Rannenberg, K., Yngström, L., Lindskog, S. (eds.) Security and Privacy in Dynamic Environments, pp. 425–430. Springer US, Boston, MA (2006)
38. Ashenden, D., Sasse, A.: CISOs and organisational culture: Their own worst enemy? Computers & Security 39, 396–405 (2013)
39. Cameron, K., Quinn, R., DeGraff, J., Thakor, A.: Competing Values Leadership. Edward Elgar Publishing (2006)
40. Wiley, A., McCormac, A., Calic, D.: More than the individual: Examining the relationship between culture and Information Security Awareness. Computers & Security 88, 101640 (2020)
41. Lin, H.-C.: An investigation of the effects of cultural differences on physicians' perceptions of information technology acceptance as they relate to knowledge management systems. Computers in Human Behavior 38, 368–380 (2014)
42. M. Karjalainen, M. Siponen, Petri Puhakainen, S. Sarker: One Size Does Not Fit All: Different Cultures Require Different Information Systems Security Interventions. In: PACIS (2013)
43. D'Arcy, J., Hovav, A., Galletta, D.: User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. Information Systems Research 20, 79–98 (2009)
44. Shaaban, H., Conrad, M.: Democracy, culture and information security: a case study in Zanzibar. Info Mngmnt & Comp Security 21, 191–201 (2013)
45. Ali, M., Brooks, L.: A situated cultural approach for cross-cultural studies in IS. Journal of Enterprise Information Management 22, 548–563 (2009)
46. Tsohou, A., Karyda, M., Kokolakis, S., Kiountouzis, E.: Formulating information systems risk management strategies through cultural theory. Info Mngmnt & Comp Security 14, 198–217 (2006)
47. Hu, Q., Dinev, T., Hart, P., Cooke, D.: Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture*. Decision Sciences 43, 615–660 (2012)
48. Knapp, K.J., Marshall, T.E., Kelly Rainer, R., Nelson Ford, F.: Information security: management's effect on culture and policy. Info Mngmnt & Comp Security 14, 24–36 (2006)
49. Werlinger, R., Hawkey, K., Beznosov, K.: An integrated view of human, organizational, and technological challenges of IT security management. Info Mngmnt & Comp Security 17, 4–19 (2009)
50. Da Veiga, A., Eloff, J.H.P.: A framework and assessment instrument for information security culture. Computers & Security 29, 196–207 (2010)
51. Dojkovski, S., Lichtenstein, S., Warren, M.: Developing information security culture in small and medium size enterprises: Australian case studies. In: ECIW2008-7th European Conference on Information Warfare and Security: ECIW2008. Reading: Academic Conferences Limited, pp. 55–66 (2008)
52. Lapke, M.: Power Relationships in Information Systems Security Policy Formulation and Implementation (2008)

53. Da Veiga, A.: The Influence of Information Security Policies on Information Security Culture: Illustrated through a Case Study. In: HAISA, pp. 22–33 (2015)
54. Johnsen, S.O., Hansen, C.W., Nordby, Y., Dahl, M.B.: Measurement and Improvement of Information Security Culture. Measurement and Control 39, 52–56 (2006)
55. Yoo, B., Donthu, N., Lenartowicz, T.: Measuring Hofstede's five dimensions of cultural values at the individual level: Development and validation of CVSCALE. Journal of international consumer marketing 23, 193–210 (2011)

Appendix A: Analyzed Articles

Table 4. Concept matrix: The influence of culture on information security policy compliance behavior. **Note**: NA = Not Applicable

The Influence of Culture on Information Security Policy Compliance Behavior				
Paper	**Level of Analysis**	**Method**	**Theory**	**Cultural Artefact**
(Hovav and D'Arcy, 2012)	National	Survey	Deterrence Theory	Hofstedes Cultural Dimensions
(Yayla, 2011)	National	Survey	Institutional Theory	Hofstedes Cultural Dimensions
(Arage et al. 2015)	National	Survey	Rational Choice Theory	NA
(Connolly et al. 2019)	National	Qualitative	NA	Hofstedes Cultural Dimensions
(Flores et al. 2014)	Organizational	Mixed Method	NA	NA
(Harris et al. 2010)	National	Survey	NA	Hofstedes Cultural Dimensions
(Flores et al. 2015)	National	Survey	Theory of planned bevahior	Hofstedes Cultural Dimensions
(AlKalbani et al. 2015)	Organizational	Survey	Technology-organization-environment (TOE) Theory	NA
(Dan and Lindström, 2011)	Organizational	Case Study (Typology)	Theory of organizational behaviour	NA
(Menard et al. 2018)	Organizational	Survey	Protection Motivation Theory	Hostedes Cultural Dimensions
(Vroom and Von Solms, 2004)	Organizational	Conceptual Framework	NA	NA
(Dinev et al. 2009a)	National	Survey	Theory of planned behavior	Hofstedes Cultural Dimensions
(Da Veiga, 2015)	Organizational	Case Study (Quantitative)	NA	NA
(Crossler et al. 2013)	NA	Comment	NA	NA
(Cockroft and Rekker, 2016)	National	Survey	NA	Hofstedes Cultural Dimensions
(Connolly et al. 2017)	Organizational	Qualitative	Deterrence Theory	NA

(Dols and Silvius, 2010)	National	Survey	NA	Hofstedes Cultural Dimensions
(Warkentin et al. 2012)	National	Survey	Deterrence Theory	Hofstedes Cultural Dimensions
(Khaled and Lane, 2008)	Organizational	Framework	NA	NA
(Hwee-Joo Kam et al. 2014)	National	Comment	Neo Institutional Theory	Hofstedes Cultural Dimensions
(Hwee-Joo Kam et al. 2015)	National	Survey	Organizational Norm Theory	Cross-Cultural Framework (CVF)
(Arage et al. 2016)	National	Survey	Rational Choice Theory	Hofstedes Cultural Dimensions
(Chen et al. 2016)	National	Survey	Protection motivation theory	Hofstedes Cultural Dimensions
(Vance et al. 2020)	National	Survey	Deterrence, Moral Beliefs, Neutralization	Hofstedes Cultural Dimensions
(Lin et al. 2020)	National	Qualitative	NA	Organizational behavior theory (Schein)
(Cram et al. 2020)	National	Meta-Analysis	NA	NA
(Da Veiga, 2016)	Individual	Survey	ISCA questionnaire	NA
(Karjalainen et al. 2020)	National	Qualitative	NA	Hofstedes Cultural Dimensions
(Amankwa et al. 2018)	Organizational	Survey	Involvement theory	Organizational behavior theory (Schein)
(Dinev et al. 2009b)	National	Survey	Theory of planned behavior	Hofstedes Cultural Dimensions
(Alfawaz et al. 2010	Organizational	Case Study (Qualitative)	Classification Theory	NA

Table 5. Concept matrix: Information security culture in organizations.
Note: NA = Not Applicable

Information Security Culture in Organizations				
Paper	**Level of Analysis**	**Method**	**Theory**	**Cultural Artefact**
(Da Veiga and Eloff, 2010)	Organizational	Conceptual Framework	NA	NA
(Amjad et al. 2017)	Organizational	Literature Review	NA	NA
(Ashenden and Sasse, 2013)	Organizational	Qualitative	NA	NA

(Da Veiga and Martins, 2017)	Individual / Subunit	Survey	NA	NA
(AlHogail, 2015)	Organizational	Conceptual Framework	NA	NA
(Lim et al. 2010)	Organizational	Case Study (Qualitative)	NA	NA
(Van Niekerk and Von Solms, 2010)	Organizational	Conceptual Framework	NA	NA
(Dhillon et al. 2016)	Organizational	Case Study (Qualitative)	Dimensions of Organizational Culture	Theory of cultural message streams
(Ruighaver et al. 2007)	Organizational	Conceptual Framework	Organizational Culture Framework	NA
(D'Arcy and Greene, 2014)	Organizational	Survey	NA	NA
(Kolkowska, 2011)	Individual / Subunit	Case Study (Qualitative)	NA	NA
(Alnatheer et al. 2012)	Organizational	Survey	NA	NA
(Lacey, 2010)	Organizational	Literature Review	NA	NA
(Ramachandran et al. 2013)	Individual / Subunit	Qualitative	NA	NA
(Dojkovski et al. 2007)	Organizational	Case Study (Mixed Method)	NA	NA
(Martins and Da Veiga , 2015)	Organizational	Survey	NA	NA
(Shuchih and Chin-Shien, 2007)	Organizational	Conceptual Framework	NA	NA
(Van Niekerk and Von Solms, 2005)	Individual / Subunit	Conceptual Framework	NA	NA
(Van Niekerk and Von Solms, 2006)	Organizational	Conceptual Framework	NA	Organizational Cultural Framework
(Zakaria, 2006)	Individual / Subunit	Conceptual Framework	NA	NA
(Alhogail and Mirza, 2014)	Organizational	Literature Review	NA	NA
(Alhogail and Mirza, 2014)	Organizational	Literature Review	NA	NA
(Alnatheer and Nelson, 2009)	Organizational	Conceptual Framework	NA	NA

(Malcolmson, 2009)	Organizational	Qualitative	NA	NA
(Ramachandran et al. 2008)	Individual / Subunit	Qualitative	NA	NA
(Schlienger and Teufel, 2003)	Organizational	Conceptual Framework	NA	Organizational Cultural Framework
(Zakaria, 2004)	Organizational	Comment	NA	Organizational Cultural Framework
(Ruighaver and Maynard, 2006)	Organizational	Conceptual Framework	NA	NA
(Thomson et al. 2006)	Organizational	Conceptual Framework	NA	NA
(Martins and Eloff, 2002)	Organizational	Conceptual Framework	NA	NA
(Da Veiga et al. 2020)	Organizational	Survey	OISCM Model	NA
(Nel and Drevin, 2019)	Organizational	Qualitative	PMT	Organizational Cultural Framework
(Tang et al. 2016)	Organizational	Case Study	NA	Hofstedes Cultural Dimensions
(Da Veiga, 2018)	Organizational	Survey	ISCA Questionnaire	NA
(Connolly and Lang, 2013)	Organizational	Mixed Method	NA	NA
(Lim et al. 2009)	Organizational	Literature Review	NA	Organizational Cultural Framework
(Ngo et al. 2005)	Organizational	Conceptual Framework	NA	NA
(Van Niekerk and Von Solms, 2013)	Organizational	Design Science	NA	Organizational Cultural Framework
(Williams, 2009)	Organizational	Conceptual Framework	NA	Organizational Cultural Framework

Table 6. Concept matrix: The influence of culture on information security awareness programs
Note: NA = Not Applicable

The Influence of Culture on Information Security Awareness Programs				
Paper	**Level of Analysis**	**Method**	**Theory**	**Cultural Artefact**
(Lin and Hsien-Cheng, 2014)	National	Survey	Theory of planned behavior	Hofstedes Cultural Dimensions
(Plachkinova and Andrés, 2015)	National	Survey	NA	Hofstedes Cultural Dimensions

(Karjalainen et al. 2013)	National	Conceptual Framework	NA	NA
(Flores et al. 2016)	Organizational	Survey	NA	NA
(Pienta et al. 2017)	Organizational	Experiment	SETA	Competing Value Framework (Cameron & Quinn 2006)
(Chen et al. 2008)	National	Experiment	NA	Hofstedes Cultural Dimensions
(Schmidt et al. 2008)	National	Survey	NA	NA
(Wiley et al. 2020)	Individual	Survey	HAIS-Q	Organizational Security Culture Measure.

Table 7. Concept matrix: The effect of culture on information security governance
Note: NA = Not Applicable

The Effect of Culture on Information Security Governance				
Paper	**Level of Analysis**	**Method**	**Theory**	**Cultural Artefact**
(Da Veiga and Eloff, 2007)	Organizational	Conceptual Framework	NA	NA
(Werlinger et al. 2009)	Organizational	Qualitative	NA	NA
(Shaaban and Conrad, 2013)	National	Mixed Method	NA	Hofstedes Cultural Dimensions
(Tsohou et al. 2006)	National	Conceptual Framework	NA	NA
(Da Veiga and Martins, 2015)	Organizational	Case Study (Quantitative)	NA	NA
(Knapp et al. 2006)	Organizational	Mixed Method	NA	NA
(Da Veiga et al. 2007)	Organizational	Survey	NA	NA
(Bess, 2009)	Organizational	Case Study (Qualitative)	Structuration Theory	NA
(Martin and Eloff, 2002)	Organizational	Conceptual Framework	NA	NA
(Okere et al. 2012)	Organizational	Qualitative	NA	NA
(Von Solms and von Solms 2004)	Organizational	Comment	NA	Schein (1992)

(Ali and Brooks, 2009)	National	Conceptual Framework	Structuration Theory	Straub 2002
(Hu et al. 2012)	Organizational	Survey	TPB	NA
(D Arcy et al. 2007)	National	Survey	Deterrence Theory	Hofstedes Cultural Dimensions
(Lapke and Dhillon, 2008)	Organizational	Case Study (Qualitative)	NA	Circuits of Power (Clegg 2002)
(Hina et al. 2020)	Organizational	Literature Review	NA	NA
(Corriss, 2010)	Organizational	Case Study (Qualitative)	Broken Window Theory	NA
(Dojkovski et al. 2007)	Organizational	Conceptual Framework	NA	NA
(Ghernaouti et al. 2010)	Organizational	Case Study (Qualitative)	NA	NA
(Johnsen et al. 2006)	Organizational	Conceptual Framework	NA	Hudson (2002)
(Luo et al. 2009)	Organizational	Survey	NA	Hofstedes Cultural Dimensions

Appendix B: Identified Articles

1. Lin, H.-C.: An investigation of the effects of cultural differences on physicians' perceptions of information technology acceptance as they relate to knowledge management systems. Computers in Human Behavior 38, 368–380 (2014)
2. Werlinger, R., Hawkey, K., Beznosov, K.: An integrated view of human, organizational, and technological challenges of IT security management. Info Mngmnt & Comp Security 17, 4–19 (2009)
3. Veiga, A.D., Eloff, J.H.P.: An Information Security Governance Framework. Information Systems Management 24, 361–372 (2007)
4. Mahfuth, A., Yussof, S., Baker, A.A., Ali, N.'a.: A systematic literature review: Information security culture. In: Social transformation through data science. ICRIIS 2017 : 5th International Conference on Research and Innovation in Information Systems : Adya Hotel, Langkawi, Kedah, 16-17th July 2017, pp. 1–6. IEEE, Piscataway, NJ (2017)
5. Da Veiga, A., Eloff, J.H.P.: A framework and assessment instrument for information security culture. Computers & Security 29, 196–207 (2010)
6. Amankwa, E., Loock, M., Kritzinger, E.: Establishing information security policy compliance culture in organizations. Info and Computer Security 26, 420–436 (2018)
7. J. Malcolmson: What is security culture? Does it differ in content from general organisational culture? In: 43rd Annual 2009 International Carnahan Conference on Security Technology, pp. 361–366 (2009)

8. Bess, D.: Understanding information security culture for strategic use: a case study. AMCIS 2009 Proceedings, 219 (2009)
9. Alnatheer, M., Nelson, K.: Proposed framework for understanding information security culture and practices in the Saudi context (2009)
10. AlHogail, A., Mirza, A.: Information security culture: A definition and a literature review. In: 2014 World Congress on Computer Applications and Information Systems (WCCAIS), pp. 1–7. IEEE (2014 - 2014)
11. AlHogail, A., Mirza, A.: A FRAMEWORK OF INFORMATION SECURITY CULTURE CHANGE. Journal of Theoretical & Applied Information Technology 64 (2014)
12. Zakaria, O.: Internalisation of Information Security Culture amongst Employees through Basic Security Knowledge. In: Fischer-Hübner, S., Rannenberg, K., Yngström, L., Lindskog, S. (eds.) Security and Privacy in Dynamic Environments, pp. 437–441. Springer US, Boston, MA (2006)
13. van Niekerk, J., Solms, R. von: Understanding Information Security Culture: A Conceptual Framework. In: ISSA, pp. 1–10 (2006)
14. van Niekerk, J., Solms, R. von: A holistic framework for the fostering of an information security sub-culture in organizations. In: Issa, 1 (2005)
15. Ernest Chang, S., Lin, C.-S.: Exploring organizational culture for information security management. Industr Mngmnt & Data Systems 107, 438–458 (2007)
16. Martins, N., da Veiga, A.: An Information Security Culture Model Validated with Structural Equation Modelling. In: HAISA, pp. 11–21 (2015)
17. Dojkovski, S., Lichtenstein, S., Warren, M.J.: Fostering information security culture in small and medium size enterprises: an interpretive study in Australia (2007)
18. Da Veiga, A.: The Influence of Information Security Policies on Information Security Culture: Illustrated through a Case Study. In: HAISA, pp. 22–33 (2015)
19. Dinev, T., Goo, J., Hu, Q., Nam, K.: User behaviour towards protective information technologies: the role of national cultural differences. Info Systems J 19, 391–412 (2009)
20. Martins, N., Da Veiga, A., Eloff, J.H.P.: Information security culture-validation of an assessment instrument. Southern African Business Review 11, 147–166 (2007)
21. McCoy, S., Galletta, D.F., King, W.R.: Integrating National Culture into IS Research: The Need for Current Individual Level Measures. CAIS 15 (2005)
22. Ramachandran, S., Rao, C., Goles, T., Dhillon, G.: Variations in Information Security Cultures across Professions: A Qualitative Study. CAIS 33 (2013)
23. Dinev, T., Goo, J., Hu, Q., Nam, K.: User behaviour towards protective information technologies: the role of national cultural differences. Info Systems J 19, 391–412 (2009)
24. Lacey, D.: Understanding and transforming organizational security culture. Info Mngmnt & Comp Security 18, 4–13 (2010)
25. Al Natheer, M., Chan, T., Nelson, K.: Understanding and measuring information security culture (2012)
26. Vroom, C., Solms, R. von: Towards information security behavioural compliance. Computers & Security 23, 191–198 (2004)
27. Pienta, D., Pu, W., Purvis, R.: The Impact of Culture on Information Security: Exploring the Tension of Flexibility and Control. In: ICIS 2017 (2017)
28. Menard, P., Warkentin, M., Lowry, P.B.: The impact of collectivism and psychological ownership on protection motivation: A cross-cultural examination. Computers & Security 75, 147–166 (2018)

29. Harnesk, D., Lindström, J.: Shaping security behaviour through discipline and agility. Info Mngmnt & Comp Security 19, 262–276 (2011)
30. Rocha Flores, W., Ekstedt, M.: Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. Computers & Security 59, 26–44 (2016)
31. Kolkowska, E.: Security subcultures in an organization-exploring value conflicts. In: ECIS 2011 Proceedings. 243. (2011)
32. D'Arcy, J., Greene, G.: Security culture and the employment relationship as drivers of employees' security compliance. Info Mngmnt & Comp Security 22, 474–489 (2014)
33. Ruighaver, A.B., Maynard, S.B., Chang, S.: Organisational security culture: Extending the end-user perspective. Computers & Security 26, 56–62 (2007)
34. AlKalbani, A., Deng, H., Kam, B.: Organisational Security Culture and Information Security Compliance for E-Government Development: The Moderating Effect of Social Pressure. In: PACIS, p. 65 (2015)
35. M. Karjalainen, M. Siponen, Petri Puhakainen, S. Sarker: One Size Does Not Fit All: Different Cultures Require Different Information Systems Security Interventions. In: PACIS (2013)
36. Rocha Flores, W., Holm, H., Nohlberg, M., Ekstedt, M.: Investigating personal determinants of phishing and the effect of national culture. Info and Computer Security 23, 178–199 (2015)
37. Dhillon, G., Syed, R., Pedron, C.: Interpreting information security culture: An organizational transformation case study. Computers & Security 56, 63–69 (2016)
38. Harris, A.L., Yates, D., Harris, J.M., Quaresma, R.: Information System Ethical Attitudes: A Cultural Comparison of the United States, Spain, and Portugal. In: AMCIS, p. 234 (2010)
39. Knapp, K.J., Marshall, T.E., Kelly Rainer, R., Nelson Ford, F.: Information security: management's effect on culture and policy. Info Mngmnt & Comp Security 14, 24–36 (2006)
40. Thomson, K.-L., Solms, R. von: Information security obedience: a definition. Computers & Security 24, 69–75 (2005)
41. Rocha Flores, W., Antonsen, E., Ekstedt, M.: Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. Computers & Security 43, 90–110 (2014)
42. van Niekerk, J.F., Solms, R. von: Information security culture: A management perspective. Computers & Security 29, 476–486 (2010)
43. Karlsson, F., Åström, J., Karlsson, M.: Information security culture – state-of-the-art review between 2000 and 2013. Info and Computer Security 23, 246–285 (2015)
44. Connolly, L.Y., Lang, M., Wall, D.S.: Information Security Behavior: A Cross-Cultural Comparison of Irish and US Employees. Information Systems Management 36, 306–322 (2019)
45. Tilahun Muluneh Arage, France Bélanger, Tibebe Beshah: Influence of National Culture on Employees' Compliance with Information Systems Security (ISS) Policies: Towards ISS Culture in Ethiopian Companies. In: AMCIS (2015)
46. da Veiga, A., Martins, N.: Improving the information security culture through monitoring and implementation actions illustrated through a case study. Computers & Security 49, 162–176 (2015)
47. Plachkinova, Miloslava and Andrés, Steven: Improving Information Security Training: An Intercultural Perspective. In: PACIS 2015 Proceedings 167 (2015)

48. Tsohou, A., Karyda, M., Kokolakis, S., Kiountouzis, E.: Formulating information systems risk management strategies through cultural theory. Info Mngmnt & Comp Security 14, 198–217 (2006)
49. Yayla, A.: ENFORCING INFORMATION SECURITY POLICIES THROUGH CULTURAL BOUNDARIES: A MULTINATIONAL COMPANY APPROACH. In: ECIS 2011 Proceedings. 243. (2011)
50. Lim, J.S., Ahmad, A., Chang, S., and Maynard, S.: Embedding Information Security Culture Emerging Concerns and Challenges. In: PACIS 2010 Proceedings. 43. (2010)
51. AlHogail, A.: Design and validation of information security culture framework. Computers in Human Behavior 49, 567–575 (2015)
52. Shaaban, H., Conrad, M.: Democracy, culture and information security: a case study in Zanzibar. Info Mngmnt & Comp Security 21, 191–201 (2013)
53. da Veiga, A., Martins, N.: Defining and identifying dominant information security cultures and subcultures. Computers & Security 70, 72–94 (2017)
54. Ashenden, D., Sasse, A.: CISOs and organisational culture: Their own worst enemy? Computers & Security 39, 396–405 (2013)
55. Arage, T., Belanger, F., Beshah, T.: Influence of National Culture on Employees' Compliance with Information Systems Security (ISS) Policies: Towards ISS Culture in Ethiopian Companies. In: AMCIS (2015)
56. Williams, P.A.: What Does Security Culture Look Like For Small Organizations? Security Research Institute (SRI), Edith Cowan University (2009)
57. van Niekerk, J., Solms, R. von: A theory based approach to information security culture change. Information (Japan) 16, 3907–3930 (2013)
58. Ngo, L., Zhou, W., Warren, M.: Understanding Transition towards Information Security Culture Change. In: AISM, pp. 67–73 (2005)
59. Luo, X., Warkentin, M., Johnston, A.C.: The impact of national culture on workplace privacy expectations in the context of information security assurance. In: AMCIS 2009, p. 521 (2009)
60. Lim, J.S., Chang, S., Maynard, S., Ahmad, A.: Exploring the Relationship between Organizational Culture and Information Security Culture. Security Research Institute (SRI), Edith Cowan University (2009)
61. Johnsen, S.O., Hansen, C.W., Nordby, Y., Dahl, M.B.: Measurement and Improvement of Information Security Culture. Measurement and Control 39, 52–56 (2006)
62. Ghernouti-Hélie, S., Tashi, I., Simms, D.: A Multi-stage Methodology for Ensuring Appropriate Security Culture and Governance. In: 2010 International Conference on Availability, Reliability and Security, pp. 353–360. IEEE (2010 - 2010)
63. Dojkovski, S., Lichtenstein, S., Warren, M.: Developing information security culture in small and medium size enterprises: Australian case studies. In: ECIW2008-7th European Conference on Information Warfare and Security: ECIW2008. Reading: Academic Conferences Limited, pp. 55–66 (2008)
64. Corriss, L.: Information security governance. In: Bishop, M. (ed.) Proceedings of the 2010 Workshop on Governance of Technology, Information and Policies - GTIP '10, pp. 35–41. ACM Press, New York, New York, USA (2010)
65. Connolly, Lena and Lang, Michael: Information Systems Security: The Role of Cultural Aspects in Organizational Settings. In: WISP 2012 Proceedings. 30. (2012)

66. Lena Connolly, M. Lang: Investigation of cultural aspects within information systems security research. 2012 International Conference for Internet Technology and Secured Transactions, 105–111 (2012)
67. Alfawaz, S., Nelson, K., Mohannak, K.: Information security culture: a behaviour compliance conceptual framework. In: Information Security 2010: AISC'10 Proceedings of the Eighth Australasian Conference on Information Security [Conferences in Research and Practice in Information Technology, Volume 105], pp. 51–60 (2010)
68. Karjalainen, M., Siponen, M., Puhakainen, P., Sarker, S.: Universal and Culture-dependent Employee Compliance of Information Systems Security Procedures. Journal of Global Information Technology Management 23, 5–24 (2020)
69. da Veiga, A.: An approach to information security culture change combining ADKAR and the ISCA questionnaire to aid transition to the desired culture. Info and Computer Security 26, 584–612 (2018)
70. Tang, M., Li, M.'g., Zhang, T.: The impacts of organizational culture on information security culture: a case study. Inf Technol Manag 17, 179–186 (2016)
71. da Veiga, A.: Comparing the information security culture of employees who had read the information security policy and those who had not. Info and Computer Security 24, 139–151 (2016)
72. Nel, F., Drevin, L.: Key elements of an information security culture in organisations. Info and Computer Security 27, 146–164 (2019)
73. Cram, W.A., D'Arcy, J., Proudfoot, J.G.: Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance. MISQ 43, 525–554 (2019)
74. Lin, C., Kunnathur, A.S., Li, L.: The Cultural Foundation of Information Security Behavior. Journal of Database Management 31, 21–41 (2020)
75. Vance, A., Siponen, M.T., Straub, D.W.: Effects of sanctions, moral beliefs, and neutralization on information security policy violations across cultures. Information & Management 57, 103212 (2020)
76. Hina, S., Dominic, P.D.D.: Information security policies' compliance: a perspective for higher education institutions. Journal of Computer Information Systems 60, 201–211 (2020)
77. da Veiga, A., Astakhova, L.V., Botha, A., Herselman, M.: Defining organisational information security culture—Perspectives from academia and industry. Computers & Security 92, 101713 (2020)
78. Wiley, A., McCormac, A., Calic, D.: More than the individual: Examining the relationship between culture and Information Security Awareness. Computers & Security 88, 101640 (2020)
79. Chen, Y., Zahedi, F.M.: Individuals' Internet Security Perceptions and Behaviors: Polycontextual Contrasts Between the United States and China. MISQ 40, 205–222 (2016)
80. Arage, T.M., Belanger, F., and Tesema, T.B.: Investigating the Moderating Impact of National Culture in Information Systems Security Policy Violation: The Case of Italy and Ethiopia" (2016). In: MCIS 2016 Proceedings. 56. (2016)
81. Kam, H.-J., Katerattanakul, P., Hong, S.-G.: A Tale of Two Cities: Information Security Policy Compliance of the Banking Industry in the United States and South Korea. University of Münster, Münster, Germany (2015)
82. Hwee-Joo Kam, Pairin Katerattanakul, Soongoo Hong: The Three Musketeers: Impacts of National Culture, Organizational Norms and Institutional Environment on Information Security Policy Compliance. In: WISP 2014 (2014)

83. K. Alshare, P. Lane: A Conceptual Model for Explaining Violations of the Information Security Policy (ISP): A Cross Cultural Perspective. In: AMCIS (2008)
84. Lapke, M.: Power Relationships in Information Systems Security Policy Formulation and Implementation (2008)
85. M. Warkentin, Nirmalee Malimage, Kalana Malimage: Impact of Protection Motivation and Deterrence on IS Security Policy Compliance: A Multi-Cultural View. In: WISP 2012 (2012)
86. T. Dols, A. Silvius: Exploring the Influence of National Cultures on Non-Compliance Behavior. Communications of the IIMA 10, 2 (2010)
87. Hovav, A., D'Arcy, J., Lee, K.: A Cross-Cultural Analysis of Security Countermeasure Effectiveness. In: WISP 2007 (2007)
88. Martins, A., Elofe, J.: Information security culture. In: Security in the information society, pp. 203–214. Springer (2002)
89. Hu, Q., Dinev, T., Hart, P., Cooke, D.: Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture*. Decision Sciences 43, 615–660 (2012)
90. Wetzels, Odekerken-Schröder, van Oppen: Using PLS Path Modeling for Assessing Hierarchical Construct Models: Guidelines and Empirical Illustration. MIS Quarterly 33, 177 (2009)
91. Yuryna Connolly, L., Lang, M., Gathegi, J., Tygar, D.J.: Organisational culture, procedural countermeasures, and employee security behaviour. Info and Computer Security 25, 118–136 (2017)
92. Cockcroft, S., Rekker, S.: The relationship between culture and information privacy policy. Electron Markets 26, 55–72 (2016)
93. Chen, C.C., Medlin, B.D., Shaw, R.S.: A cross-cultural investigation of situational information security awareness programs. Info Mngmnt & Comp Security (2008)
94. Ali, M., Brooks, L.: A situated cultural approach for cross-cultural studies in IS. Journal of Enterprise Information Management 22, 548–563 (2009)
95. Thomson, K.-L., Solms, R. von, Louw, L.: Cultivating an organizational information security culture. Computer Fraud & Security 2006, 7–11 (2006)
96. Ruighaver, A.B., Maynard, S.B.: Organizational Security Culture: More Than Just an End-User Phenomenon. In: Fischer-Hübner, S., Rannenberg, K., Yngström, L., Lindskog, S. (eds.) Security and Privacy in Dynamic Environments, pp. 425–430. Springer US, Boston, MA (2006)
97. Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., Baskerville, R.: Future directions for behavioral information security research. Computers & Security 32, 90–101 (2013)
98. Zakaria, O.: Understanding Challenges of Information Security Culture: A Methodological Issue. In: AISM, pp. 83–93 (2004)
99. Solms, R. von, Solms, B. von: From policies to culture. Computers & Security 23, 275–279 (2004)
100. Schlienger, T., Teufel, S.: Information security culture-from analysis to change. South African Computer Journal 2003, 46–52 (2003)
101. Ramachandran, S., Rao, S.V., Goles, T.: Information Security Cultures of Four Professions: A Comparative Study. In: Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008), p. 454. IEEE (2008 - 2008)
102. Okere, I., van Niekerk, J., Carroll, M.: Assessing information security culture: A critical analysis of current approaches. In: 2012 Information Security for South Africa, pp. 1–8 (2012)
103. Martins, A., Eloff, J.: Assessing Information Security Culture. In: ISSA, pp. 1–14 (2002)

Culture Matters - A Cross Cultural Examination of Information Security Behavior Theories

Sebastian Hengstler[1]

[1] Chair of Information Security and Compliance, University of Goettingen, Germany
s.hengstler@stud.uni-goettingen.de

Abstract. Ensuring information security is an international problem and poses particular challenges for international companies. Research proposes various solutions for ensuring information security based on several theories such as the deterrence theory or the protection motivation theory. What is currently missing is a comparison of these theories in an intercultural context to test their comparability and different effectiveness. In our study, we empirically tested the theories and determined their comparability with invariance testing and predictive power between Germany, India and the USA using a SEM approach. Our results show differences in the effectiveness of the theoretical models across the three cultures. The results provide initial insights into the use of the theories in an international context and offer a practical approach to design culture-specific security measures

Keywords: Information Security Policy Compliance Behavior, Cross-cultural research, Deterrence Theory, Protection Motivation Theory

1 Introduction

With the increasing relevance of information security for ensuring successful business in the digital age, the need for effective measures to ensure secure employee behavior within organizations is growing [1]. As a basis for ensuring security behavior, companies define information security policies (ISP). ISPs are defined as "a set of formalized procedures, guidelines, roles and responsibilities to which employees are required to adhere to safeguard and use properly the information and technology resources of their organizations [2]". Research on ISP compliance behavior (ISPCB) has already been developed a variety of contextualized theories to explain employee behavior, mainly using theories from other disciplines such as sociology, psychology, criminology or health care [3]. These approaches provide detailed insights into how ISPCB can be explained and influenced positively or negatively and helps in practice to design effective security measures [4].

However, the results of current research still highlight some less considered problems such as the analysis of cultural differences in ISPCB [5, 6]. This becomes particularly relevant when internationally operating companies want to define their security measures and use them in their heterogeneous cultural environment [7].

16th International Conference on Wirtschaftsinformatik,
March 2021, Essen, Germany

Existing research partially considers this problem when analyzing ISPCB [3, 8]. Previous research shows, for example, that the effectiveness of established measures to ensure information security can vary from one national culture to another [7]. Other culture-related studies analyze the cultural differences in information security attitudes and behavior of employees [9].

Thus, there is still a need for the examination of aspects that have not yet been taken into account to a sufficient extent. First, the current research describes that only a limited set of cultures have been analyzed at the national level for differences in terms of ISPCB [5, 10]. Second, existing approaches either do not use theories to describe cultural differences regarding ISPCB in their basic form or consider specific contexts, such as different security offenses [8, 11]. An analysis of theoretical mechanisms in a general ISPCB context offer the possibility of better comparability and more specific use of the results with existing and future research [12]. Currently, we cannot say whether current analyzed theories in ISPCB research differ in their predictive power and mechanisms in different countries because there is no common level of comparability. Therefore, the aim of this study is to investigate whether the predictive power of established theories and their mechanisms differ in different national cultures.

Our study addresses the mentioned gaps as follows. Using two of the most widely used theories in ISPCB research, the Deterrence Theory (DT) [8] and the Protection Motivation Theory (PMT) [13] we collected, analyzed and compared data sets with different cultural values from Germany, the USA and India using an SEM-PLS approach. We use the two theories mentioned above because they have different perspectives on ISPCB [3]. Our analysis comprises of three aspects. First, we conduct invariance testing to validate that the measurement instruments measure the same theoretical construct across our cultures. Second, there is an established tradition in information systems research in general, of comparing research models that have been developed and tested in earlier work [14]. Thus, we follow this approach and compare the predictive power and the mechanisms of the two theories [15]. We test for statistical differences between the explained variance in ISPCB using a Multi Group Analysis.

The rest of the paper is structured as follows. In the second section, we look at the cultural dimensions that are the basis for our cross-cultural comparison and describe the analyzed theories DT and PMT. We then develop the research model and present the explorative hypotheses underlying this study in the third section. Subsequently, the results of the study are presented. The study concludes with a discussion, limitations, contributions and an outlook on further research potentials.

2 Theoretical Background

2.1 The Concept of National Culture

The factor culture is an essential dimension that shapes an individual's behavior and can be described as a summary of ideologies, beliefs, basic assumptions, shared norms and values, that have an influence on the collective will [16]. Existing research on

information security and culture indicates a wide range of studies in which the influence of theoretical mechanisms on ISPCB are analyzed, based on national cultural differences. To apply these cultural differences, Hofstede's cultural dimensions provide a solid base for a comparison and are a widely used approach in information security research [9]. The dimensions consist of the constructs power distance (PD), uncertainty avoidance (UA), individualism/collectivism (COL), Masculinity/Femininity (MAS) and long-term orientation (LO). Power distance determines the degree to which people accept and expect that power is distributed unequally. Uncertainty Avoidance defines the degree to which people feel uncomfortable with uncertainty and ambiguity. Individualism is defined as a preference of individuals to take care of only themselves and their families. Collectivism is the opposite. Masculinity and Femininity can be related to tough vs. Tender cultures. According to Hofstede (2011) Masculinity represents values ass heroism, material rewards or success. Femininity is related to the preference for cooperation, modesty and quality of life. This orientation defines the degree to which long term values and traditions are balanced in contrast to thrift encouragement and efforts in modern solutions [17]. We used Hofstede's cultural dimensions for two reasons. First, the dimensions have been rigorously developed and provide definitions for different cultural dimensions. Second, their application allows us to better integrate our theoretical findings in this stream of literature [7].

Table 1**.** Comparison of Cultural Dimensions between Nations

Cultural Dimension	**Country Score**		
	Germany	USA	India
Power Distance	35	40	77
Uncertainty Avoidance	65	46	40
Collectivism	67	91	48
Masculinity/Femininity	66	62	56
Long Term Orientation	31	29	61

We selected these three nations Germany, India and USA because, they have different values in Hofstede's cultural dimensions and thus, form a good basis for analyzing cultural differences at the national level. Table 1 shows that India has a higher value for PD than Germany or the USA, which means in the Indian culture it is more likely to accept the unequal distribution of power than in the national culture of Germany or the USA. Uncertainty avoidance differs more between Germany and the USA and India, which shows that in German culture uncertainty and ambiguity are described as more uncomfortable than in the U.S. and India. The COL dimension is strongest for the USA and lowest for India. It shows that the national culture of the U.S.A has a strong bias for collective action in society instead of emphasizing individualism. The dimension MAS shows similarly high values in all three cultures. LO is more pronounced in India than in the USA or Germany and shows that Indian culture

emphasizes long-term values and traditions instead of thrift encouragement and efforts in modern solutions. Overall, the three national cultures show a good distribution in the characteristics of the cultural dimensions according to Hofstede and are therefore well suited for carrying out an intercultural comparison at the national level.

2.2 Deterrence Theory in Information Security Research

The DT has its origin in criminology and has been widely used in information security research [8]. The theory states that individuals will choose to commit an offence, if the benefits outweigh the underlying penalties. The DT further describes that the trade-off between benefits and the expected penalty can be further divided in different mechanisms, namely sanction certainty, sanction severity and sanction celerity [11]. When considering the DT in existing information security literature, a wide range of uses can be identified. The application of the original form of DT concentrates on the usage of formal sanctions to explain ISPCB, while other research additionally includes more informal consequences, such as informal sanctions like guilt and shame. Formal sanction severity is described as the formal expected amount of a penalty when a policy violation is committed, such as a fine or a warning, while an example for informal sanction severity could the loss of reputation among colleagues and superiors or shame. Formal sanction certainty describes the perceived probability of being formally punished if one is caught for an ISP non-compliant behavior, while informal sanction certainty describes probability of being informally punished by the social environment (e.g. at the workplace) [3]. Sanction celerity describes the velocity a person is punished if a crime was committed [18].
Both formal and informal sanction certainty and sanction celerity find empirical support in various contexts of information security research [19]. Since sanction severity and sanction celerity are considered as the two main components of deterrence theory, since celerity has received less empirical support in information security research so far, we only considered formal and informal sanction severity and sanction celerity in our research model [11].

2.3 Protection Motivation Theory in Information Security Research

The PMT has its origins in healthcare research. The theory states that a person, when confronted with a threat, cognitively weighs the threat and a possible related protective measure [20]. After assessing the threat and potential countermeasures to cope with it, the individual decides to adopt an adaptive or non-adaptive behavior. Adaptive behaviors are recommended responses designed to protect against a threat, whereas non-adaptive responses involve behaviors in which the threat recipient avoids implementing a recommended response. PMT assumes that the susceptibility to threats and the severity of the threat have a positive effect on a person's behavior and adaptation. Similarly, in its adapted form, the PMT contains further constructs used to constitute the protection motivation, such as response effectiveness, self-efficacy to comply and response costs, which have a direct influence on behavior [21]. Response cost describe the perceived extrinsic or intrinsic personal costs of performing the

suggested adaptive behavior in terms of time, money or effort. Response efficacy is described as the perceived effectiveness of the behavior in mitigating or avoiding the perceived violation. Self-efficacy is defined as the confidence an individual possesses in effectively performing a recommended response and to complying with given ISP's. Severity is defined as the perceptions of the seriousness of an information security violation. Susceptibility refers to the degree to which someone feels vulnerable to a specific violation of ISP's [13].

The constructs of the PMT find broad empirical support in information security research. Menard et al. (2017) analyze the impact of PMT on the individual motivation of information technology users. Johnston and Warkentin (2010) developed their fear-appeal model based on the PMT in order to convey the effectiveness of an antispyware software [22]. Moody et al. (2018) show that PMT constructs such as response efficacy, severity and susceptibility have an indirect effect on behavior [3]. However, current information security research lacks on studies on the relationship between PMT constructs and national culture [13, 20]. We, therefore, used the explained theoretical constructs of the PMT for our cross-cultural analysis.

3 Research Approach

3.1 Hypotheses development and Research Design

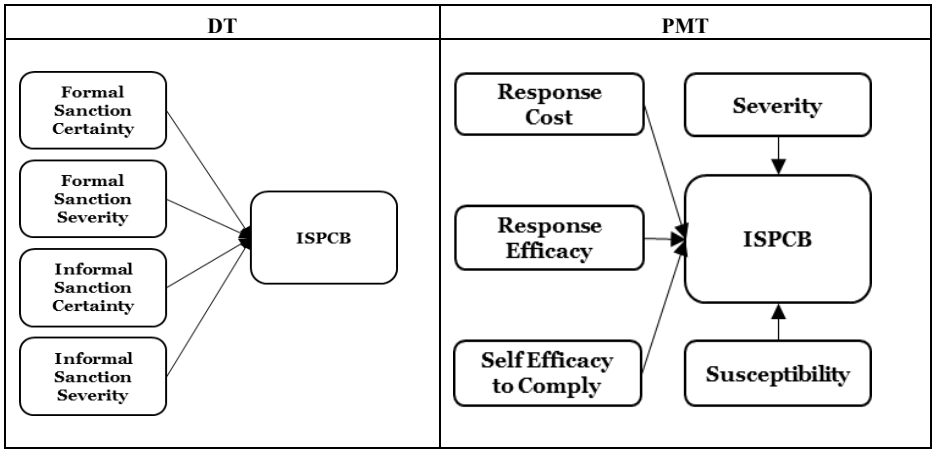
The hypotheses of a research project serve to answer the underlying research questions. However, in order to answer our research questions, we need to operationalize the theories we have introduced earlier in our study. The construct definitions from the DT and PMT were used to transfer the theories into a structural model displayed in Figure 1. This becomes necessary because the results of the structural model are needed to determine the effect strengths of the respective theory components on ISPCB. They are used to determine the predictive power of the theories for ISPCB. We furthermore analyze different effect sizes between the constructs along different cultures to identify significant differences as it has been shown that differences in cultural values can have an influence on behavior [17]. We draw on this argumentation and propose the following hypotheses:

H1: The predictive power of DT and the model's mechanisms differ across cultures.
H2: The predictive power of PMT and the model's mechanisms differ across cultures.

We conducted an empirical cross-cultural study to examine our underlying hypotheses. The operationalization of their variables follows a context-independent approach, measuring general ISPCB in order to make more generalized statements about the effectiveness of the theories and to compare their explanatory power throughout the culture samples [12]. For the measurement of behavior, the items of D'Arcy and Lowry (2019) were used and generalized for our study. Furthermore, we used 7-point Likert scales for our questionnaires. The items for formal and informal

sanction severity and -certainty of the DT (3 items each) were adapted by Moody et al. (2018) and rephrased for our study [3]. The items used for the constructs response cost and response efficacy of the PMT were adapted by Floyd et al. (2000) (4 items each). Self-efficacy, severity and susceptibility were taken from Menard et al. (2017) and adapted (3 items each) [13, 20]. The used questions per item are listed in the appendix.

Figure 1. Research Models of DT and PMT.



We used an SEM approach and the partial least squares (PLS) method to test the theoretical models, because it has fewer sample size requirements and is characterized by excellent prediction [24]. We performed a cross-model comparison by using a multi-group analysis (MGA) to look for significant differences in the mean differences of the explained variance of our models across our samples as well as in the path coefficients of the analyzed theories (Welch-Satterthwait test) [25].

3.2 Data collection, Sample Characteristics and Common-Method Bias

A pilot study was conducted by sending the survey to five academic experts for review. A test run was then started with 60 participants for each sample, where at least 30 results per sample were complete and valid. The crowdsourcing platforms Amazon Mechanical Turk and Clickworker were used to collect the data, taking into account the quality criteria for using crowd working platforms, defined by Lowry et al. (2016) [26]. Only participants with their cultural background and origin from the respective sample (USA, India, Germany) were able to participate in our study. Their job acceptance rate on the platform must have been higher than 90%, and a certification of English language skills must be registered on the platform. We only selected participants which were employed, worked at least partially with a computer in their job and whose organization had an ISP. Additional attention checks were built into the study (e.g., requests to select a specific response) to avoid systematic response patterns. Participants were paid $1.65 for successful and conscientious participation in the study. In total, 767 people participated in the German survey, 623 in the survey within the USA and 481 people in

the Indian survey. After applying the used quality criteria, the resulting samples consist of 422 (57%) valid responses collected in Germany, 263 (42%) in the USA and 252 (52%) in India. Demographic characteristics of the respondents were adapted from Hovav and D'Arcy (2012). The average age in all three countries is between 30 and 35 years. In all three countries, the proportion of men is higher than 60%. The majority of the participants work in a company with more than 1000 employees.

To carry out the common method bias test, we used the marker variable technique [27] and chose the respondent's outside activities as the theoretically unrelated marker variable [23]. The highest variance that the marker shares with another construct is less than 0.05. In addition, the path coefficients between the constructs showed no significant size changes (> 0.01 and not significant). In conclusion, the result suggests that there is no evidence of a common method bias in our study.

4 Data Analysis and Results

4.1 Measurement Models and Invariance Testing

To check our data for reliability, common quality criteria for reflective measurement models in IS research were applied to our study [28]. We used individual item reliability, composite construct reliability (CR), and average variance extracted (AVE) as indicators of convergent validity for our models. The factor loadings of the items for the DT and PMT model were all above 0.70, which indicates sufficient item reliability [29] (see appendix). The CR is higher than 0.70 for every variable used in each model, and the AVE is higher than 0.5 [28]. We furthermore used the Fornell and Larcker criterion to confirm discriminant validity by showing that for each model, the AVE for each construct is higher than the variance shared with other constructs (see square root AVEs as bold numbers in Table 2). [30, 31]. In summary, our results indicate that our measurement model is acceptable and reliable.

Table 2. Inter-construct correlations, construct reliability, and average variance extracted of Deterrence Theory Model.

Samples and Items		CR	AVE	FSC	FSS	ISC	ISS	ISPCB
Germany	**FSC**	0.884	0.719	**0.848**				
	FSS	0.917	0.786	0.581	**0.887**			
	ISC	0.913	0.778	0.468	0.496	**0.882**		
	ISS	0.919	0.79	0.409	0.551	0.649	**0.889**	
	ISPCB	0.938	0.834	0.347	0.318	0.428	0.378	**0.913**
USA	**FSC**	0.85	0.654	**0.809**				
	FSS	0.87	0.693	0.618	**0.832**			
	ISC	0.903	0.757	0.404	0.447	**0.87**		
	ISS	0.881	0.713	0.366	0.451	0.667	**0.844**	
	ISPCB	0.918	0.789	0.399	0.373	0.394	0.491	**0.888**

India	**FSC**	0.808	0.585	**0.765**					
	FSS	0.823	0.608	0.5	**0.78**				
	ISC	0.841	0.639	0.344	0.359	**0.799**			
	ISS	0.801	0.576	0.408	0.624	0.507	**0.759**		
	ISPCB	0.823	0.609	0.453	0.433	0.357	0.475	**0.78**	
Samples and Items		**CR**	**AVE**	**RC**	**REF**	**SEF**	**SEV**	**SUS**	**ICB**
Germany	**RC**	0.866	0.624	**0.79**					
	REF	0.906	0.708	-0.015	**0.842**				
	SEF	0.931	0.819	-0.167	0.328	**0.905**			
	SEV	0.918	0.788	0.155	0.197	0.095	**0.888**		
	SUS	0.944	0.85	-0.084	0.346	0.400	0.339	**0.922**	
	ISCPB	0.866	0.624	-0.162	0.333	0.495	0.074	0.467	**0.913**
USA	**RC**	0.926	0.759	**0.871**					
	RE	0.887	0.664	-0.199	**0.815**				
	SEF	0.916	0.784	-0.237	0.499	**0.885**			
	SEV	0.915	0.781	0.414	0.088	-0.003	**0.884**		
	SUS	0.905	0.761	-0.082	0.476	0.500	0.131	**0.872**	
	ISPCB	0.918	0.789	-0.263	0.597	0.603	-0.009	0.539	**0.888**
India	**RC**	0.87	0.628	**0.792**					
	REF	0.805	0.509	0.35	**0.714**				
	SEF	0.81	0.588	0.138	0.47	**0.767**			
	SEV	0.841	0.64	0.395	0.437	0.395	**0.8**		
	SUS	0.787	0.553	0.234	0.516	0.531	0.402	**0.743**	
	ISPCB	0.824	0.609	0.161	0.543	0.698	0.331	0.606	**0.781**

Notes (also for following tables): **FSC** = Formal Sanction Certainty. **FSS** = Formal Sanction Severity. **ISC** = Informal Sanction Certainty. **ISS** = Informal Sanction Severity. **RC** = Response Cost. **REF** = Response Efficacy. **SEF** = Self Efficacy. **SEV** = Severity. **SUS** = Susceptibility. The bold numbers on the leading diagonal are the square root of the AVE. *significant at 0.1; ** significant at 0.05; *** significant at 0.01.

Additionally, we tested for configural and metric measurement invariance. This step is necessary to create the ability to further analyze differences in the predictive power of the theories in a cross cultural manner [32]. Only if the charges of the similar items are invariant across groups, differences in the item scores can be meaningfully compared to the extent that they indicate similar group differences in the underlying construct [33]. To measure invariance, we performed a MGA and tested the differences in item loadings for all models between the three samples. We were not able to find significant differences between the item loadings of our samples and thus show metric invariance and comparability of our results.

4.2 Testing Theoretical Mechanisms across Cultures

We have tested the previously introduced path models with the PLS algorithm for estimating the structural model. We used the bootstrapping method to determine the significance of the path coefficients with 5000 bootstrap samples [28]. An overview of

our significance levels of the individual path coefficients for all three models is given in Table 3.

Table 3. Structural Models of DT and PMT Research Model.

Model Path	Germany	USA	India	Germany / USA	Germany / India	USA / India
	Path Coefficients			**Significant Effect Differences**		
Deterrence Theory						
FSC -> ISPC	0.150***	0.211***	0.252***	NS	NS	NS
FSC -> ISPCB	0.018	0.052	0.124*	NS	NS	NS
ISC -> ISPCB	0.196***	0.058	0.105	S*	NS	NS
ISS -> ISPCB	0.164***	0.372***	0.213***	S*	NS	NS
Protection Motivation Theory						
RC -> ISPCB	-0.049	-0.086*	-0.011	NS	NS	NS
REF -> ISPCB	0.149***	0.307***	0.207***	S*	NS	S**
SEF -> ISPCB	0.324***	0.296***	0.467***	NS	S*	S*
SEV -> ISPCB	-0.062	-0.033	-0.049	NS	NS	NS
SUS -> ISPCB	0.279***	0.220***	0.279***	NS	NS	NS

While formal sanction certainty and informal sanction severity have a significant impact in all three models, formal sanction severity only applies to India and informal sanction certainty only to Germany. The mechanisms of PMT are almost equally applicable to all three cultures. While response efficacy, self-efficacy and susceptibility are applicable in all three models and severity has no significant effect in all of them, response cost is only significantly applied in the USA model.

We additionally identified some significant effects of our control variables (see appendix). Age has a significant effect on ISPCB in at least one of the samples for each theory. The company size and industry only have an influence in the DT model. Education affects at least one sample for each theory. For gender, only one significant effect can be found in the PMT model.

4.3 Comparing the Predictive Power across Cultures

In order to determine the predictive power of the theories and then compare them, we first considered the path coefficients of the individual models and determined whether significant differences exist in their height [25]. In the second step we compared the explained variance and also investigated whether significant differences exist. As analyzed in the previous chapter, different significances can be identified in the path coefficients of the DT models. However, it can be observed that only significant path differences can be identified in the informal sanctions. For example, ISC in the USA model is significantly higher than in the German model (significant at 0.1). The same

difference can be found for ISS. The PMT model was tested using five different constructs. Response efficacy has a significant effect on ISPCB in all three models, whereas the effect in the USA is significantly higher than in Germany and India. There is a significant effect of self-efficacy on ISPCB in all models where the path coefficient in the Indian is significantly higher as in the USA and German one (significant at 0.1).

When interpreting the explained variance, the acceptable values depend on the research context [29]. In general, a proportion of the explained variance of an endogenous variable is considered low up to 0.32, moderate from 0.33 and substantial from 0.67. The R^2 adjusted in the DT model is in the medium range for the USA (0.350) and India (0.327), for the German sample slightly below the 0.32 limit at 0.291. However, the MGA showed that the difference between Germany and USA and Germany and India is significant (significant at 0.05). For the PMT models, all R^2 adjusted are in the medium range, whereas only the value for Germany is below 0.4 (0.358) and significantly different compared to the USA (0.520) and Indian (0.580) sample (significant at 0.05). The R^2 adjusted values for the PMT and DT model are above average [8]. The differences in the R^2 values may result from the different operationalisation of the theories, as we use basic models or have no further context-specific extensions in our models. Along the investigated theories we can see that there are significant differences in the path coefficients of the theories as well as in the R^2 of the models.

5 Discussion

5.1 Implications for Research and Practice

Our results show implications for research as well as for practice. The main purpose of this analysis was to empirically evaluate and compare the predictive power of the DT and PMT along three different national cultures. The results of the analysis provide different insights into the cultural differences when applying the theories and show interesting theoretical contributions. First, by applying configural and metric invariance between our cultural samples, we can show that our used models and items of the DT and PMT are understood in the same way across different cultures [33]. These results are the basic prerequisite for a comparison of the theories between the national cultures. Secondly, we were able to show that there are differences in the predictive power of DT and PMT mechanisms. We could show for our context that the theories have a small to medium-strong explanatory power. Significant differences along the cultures exist in the DT model between USA and Germany. In addition, we were able to show in our study that the PMT constructs response efficacy and self-efficacy explains the ISPCB significantly better in India and the USA than in Germany. Furthermore, our results show different effects for the effectiveness of formal sanctions in the USA than in existing research [7]. Our results provide important information on the effectiveness of models on ISPCB in order to define what types of measures are appropriate to ensure ISPCB in an international context. These findings indicate that ISPCB research needs to consider cultural differences in the use of DT and PMT. Our results provide a basis

for more specific investigation, such as analysing the effects of individual cultural dimensions on the mechanisms of the theories analysed. Finally, we can contribute to a broader consideration of intercultural comparisons between more than two nations since we integrated national samples such as Germany and India which were previously less considered in cross-cultural research of ISPCB [6].

Practitioners can also benefit from the conclusions of our results. Our findings underline the relevance of a cultural differentiation of measures for the management of security breaches. Overall, in the future, it will be important to consider cultural differences when using security measures to positively influence ISPCB. Companies should pay attention to the fact that the measures work differently in different international locations. They should be designed with a culture-specific mode of operation in mind. An example of such differences is the use of sanctions. While our results show that the severity of an expected formal punishment in different cultures tends to be less effective ISPCB, the sole high probability that a formal punishment is to be expected is comparatively more effective.

5.2 Limitations and Future Research

For an adequate interpretation of our results, the following limitations of the study should be considered. On the one hand, we measured general ISPCB and did not specifically refer to one or more contexts. The general validity of our results cannot be proven by the fact that cultural differences can be context specific. Future research can take up this aspect and examine our results as a starting point for cultural differences in specific ISPCB contexts. Secondly, in order to compare different cultures, we have used three example cultures, which differ in their cultural dimensions according to [17]. Thus, our results are limited to the cultures we selected. In order to find out more about the differences between cultures, we need to involve further culture samples and take a closer look at the direct influences of cultural dimensions on specific behaviour. Furthermore, we could not consider the problem of a cultural shift in detail. For example, our samples from the different countries could be influenced by the individual cultural values of each subject. In order to obtain a detailed consideration of cultural values on the studied theoretical constructs and ISPCB, future studies should also measure culture on an individual level and investigate it in terms of its influence on ISPCB. [7]. Third, moderating factors could only partially be addressed in our work. More detailed differences and the involvement or deepening of other factors, such as an industry-specific investigation or an analysis based on different educational backgrounds, will be subjected to future research.

6 Conclusion

Studies on the analysis of ISPCB often show the need to consider their results from different cultural perspectives. However, existing studies in this area rarely take an empirical approach, look at given problems from different theoretical lenses and put the results into context. This study is the first to empirically test and compare three

prominent theories that are often used to explain ISPCB. Furthermore, we were able to identify different types of effects in different cultures and that their effect strength can vary. Interestingly, both strong similarities and differences can be identified across theories. Other interesting aspects are constant effects along the three cultures analyzed, such as attitude or susceptibility as an effective factor for explaining ISPCB. Our results give a first impression of cultural differences in the effectiveness of different theoretical models and provide a starting point for the design and implementation of ISP's in an international environment. In summary, future research on ISPCB and culture should be based on these results when deciding for or against a theoretical lens and should conduct more specific analyses.

References

1. Barlow, J.B., Warkentin, M., Ormond, D., Dennis, A.R.: Don't Even Think About It! The Effects of Antineutralization, Informational, and Normative Communication on Information Security Compliance. Journal of the Association for Information Systems 19 (2018)
2. Lowry, P.B., Moody, G.D.: Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. Info Systems J 25, 433–463 (2015)
3. Moody, G.D., Siponen, M., Pahnila, S.: Toward a Unified Model of Information Security Policy Compliance. MIS Quarterly 42, 285–311 (2018)
4. Willison, R., Warkentin, M., Johnston, A.C.: Examining employee computer abuse intentions: insights from justice, deterrence and neutralization perspectives. Info Systems J 28, 266–293 (2018)
5. Cram, W.A., D'Arcy, J., Proudfoot, J.G.: Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance. MISQ 43, 525–554 (2019)
6. Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., Baskerville, R.: Future directions for behavioral information security research. Computers & Security 32, 90–101 (2013)
7. Hovav, A., D'Arcy, J.: Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. Information & Management 49, 99–110 (2012)
8. Trang, S., Brendel, B.: A Meta-Analysis of Deterrence Theory in Information Security Policy Compliance Research. Inf Syst Front 21, 1265–1284 (2019)
9. Connolly, L.Y., Lang, M., Wall, D.S.: Information Security Behavior: A Cross-Cultural Comparison of Irish and US Employees. Information Systems Management 36, 306–322 (2019)
10. Chen, Y., Zahedi, F.M.: Individuals' Internet Security Perceptions and Behaviors: Polycontextual Contrasts Between the United States and China. MISQ 40, 205–222 (2016)
11. D'Arcy, J., Herath, T.: A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. European Journal of Information Systems 20, 643–658 (2011)

12. Aurigemma, S., Mattson, T.: Generally Speaking, Context Matters: Making the Case for a Change from Universal to Particular ISP Research. Journal of the Association for Information Systems (2019)
13. Menard, P., Bott, G.J., Crossler, R.E.: User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory. Journal of Management Information Systems 34, 1203–1230 (2017)
14. Srite, Karahanna: The Role of Espoused National Cultural Values in Technology Acceptance. MISQ 30, 679 (2006)
15. Brown, S.A., Venkatesh, V., Hoehle, H.: Technology adoption decisions in the household: A seven-model comparison. J Assn Inf Sci Tec 66, 1933–1949 (2015)
16. Leidner, D.F., Kayworth, T.: Review: a review of culture in information systems research: toward a theory of information technology culture conflict. MIS Quarterly 30 (2006)
17. Hofstede, G.: Culture's consequences. Comparing values, behaviors, institutions, and organizations across nations. Sage Publ, Thousand Oaks, Calif. (2011)
18. Vance, A., Siponen, M.T., Straub, D.W.: Effects of sanctions, moral beliefs, and neutralization on information security policy violations across cultures. Information & Management 57, 103212 (2020)
19. Willison, R., Lowry, P.B., Paternoster, R.: A Tale of Two Deterrents: Considering the Role of Absolute and Restrictive Deterrence to Inspire New Directions in Behavioral and Organizational Security Research. JAIS, 1187–1216 (2018)
20. Floyd, D.L., Prentice-Dunn, S., Rogers, R.W.: A Meta-Analysis of Research on Protection Motivation Theory. Journal of Applied Social Psychology 30, 407–429 (2000)
21. M. Warkentin, N. Malimage, K. Malimage: Impact of Protection Motivation and Deterrence on IS Security Policy Compliance: A Multi-Cultural View. In: WISP 2012 (2012)
22. Johnston, Warkentin: Fear Appeals and Information Security Behaviors: An Empirical Study. MIS Quarterly 34, 549 (2010)
23. D'Arcy, J., Lowry, P.B.: Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. Info Systems J 29, 43–69 (2019)
24. Ringle, S., Straub, S.: Editor's Comments: A Critical Look at the Use of PLS-SEM in "MIS Quarterly". MIS Quarterly 36, iii (2012)
25. Rocha Flores, W., Antonsen, E., Ekstedt, M.: Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. Computers & Security 43, 90–110 (2014)
26. Lowry, P.B., D'Arcy, J., Hammer, B., Moody, G.D.: "Cargo Cult" science in traditional organization and information systems survey research: A case for using nontraditional methods of data collection, including Mechanical Turk and online panels. The Journal of Strategic Information Systems 25, 232–240 (2016)
27. Lindell, M.K., Whitney, D.J.: Accounting for common method variance in cross-sectional research designs. Journal of Applied Psychology 86, 114–121 (2001)
28. Hair, J.F., Hult, G.T.M., Ringle, C.M., Sarstedt, M.: A primer on partial least squares structural equation modeling (PLS-SEM). SAGE, Los Angeles, London, New Delhi, Singapore, Washington DC, Melbourne (2017)

29. Hair, J.F.: A primer on partial least squares structural equation modeling (PLS-SEM). Sage Publ, Los Angeles (2014)
30. Chin, W.: Issues and Opinion on Structural Equation Modeling. MIS Quarterly 22 (1998)
31. Fornell, C., Larcker, D.F.: Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. Journal of Marketing Research 18, 39 (1981)
32. Steelman, Z.R., Hammer, B.I., Limayem, M.: Data Collection in the Digital Age: Innovative Alternatives to Student Samples. MISQ 38, 355–378 (2014)
33. Henseler, J., Ringle, C.M., Sarstedt, M.: Testing measurement invariance of composites using partial least squares. International Marketing Review 33, 405–431 (2016)

Appendix

Table 4. Analyzed Control Variables.

Control Variables	**Deterrence Theory**			**Protection Motivation Theory**		
	Germany	USA	India	Germany	USA	India
Age	0.269***	0.138***	0.099*	0.057*	0.096**	0.029
Company Size	0.102***	0.008	0.037	0.013	-0.02	-0.017
Education	0.035	-0.138***	-0.061	0.099***	0.034	0.011
Gender	0.059	0.036	-0.026	0.065*	0.037	0.067*
Industry	0.120***	0.144***	0.132***	0.032	0.033	-0.031
Job Position	0.012	-0.033	0.024	-0.071	0.044	0.035

Table 5. Used Items.

Construct	Item
Formal Sanction Severity	1. How much of a problem would it create in your life if you violated the company information security policy? 2. How much of a problem would it be if you received severe sanctions if you violated the company information security policy? 3. How much of a problem would it create in your life if you were formally sanctioned if you violated the company information security policy?
Formal Sanction Certainty	1. What is the chance that you would be formally sanctioned (punished) if management learned that you had violated company information security policies? 2. I would receive corporate sanctions if I violated company ISP procedures. 3. What is the chance that you would be warned if management learned you had violated company information security procedures?
Informal Sanction Severity	1. It would create a problem in my life if my career was adversely affected for not complying with ISP procedures regularly. 2. It would create a problem in my life if I lost the respect and good opinion of my colleagues for not following ISP procedures regularly.

	3. It would create a problem in my life if I lost the respect of my manager for not complying with ISP procedures regularly.
Information Sanction Certainty	1. How likely is it that you would lose the respect and good opinion of your business associates for violating company information security procedures? 2. How likely is it that you would jeopardize your promotion prospects if management learned that you had violated company information security procedures? 3. How likely is it that you would lose the respect and good opinion of your manager for violating company information security policies?
Response Cost	1. Complying with information security procedures would be time consuming. 2. Complying with information security procedures would take work time. 3. Complying with information security procedures makes my work more difficult. 4. Complying with information security procedures inconveniences my work.
Response Efficacy	1. Complying with information security procedures in our organization keeps information security breaches down. 2. If I were to comply with information security procedures, IS security breaches would be scarce. 3. If I were to do the opposite to what Mattila did, it would keep IS security breaches down. 4. If I were to do the opposite to what Mattila did, IS security breaches would be minimal.
Self-Efficacy to Comply	I have the necessary ... to fulfil the requirements of the ISP (skills, knowledge, competencies).
Severity	An information security breach in my organization would be serious / severe / significant.
Susceptibility	1. My information and technology resources are at risk for becoming attacked. 2. It is likely that my information and technology will become compromised. 3. It is possible that my information and technology resources will become compromised.
ISPCB	1. I complied with the requirements of the ISP. 2. I protected information and technology resources according to the requirements of the ISP. 3. I carried out my responsibilities prescribed in the ISP when I used information and technology.

MIA - A Method for Achieving Compliance in Flexible and IT Supported Business Processes (Extended Abstract)

Tobias Seyffarth[1]

[1]Martin Luther University Halle-Wittenberg, Chair of Information Management, Halle (Saale), Germany
tobias.seyffarth@wiwi.uni-halle.de

Keywords: business process; compliance; change; IT architecture

1 Motivation

Compliance describes the adherence to compliance requirements, which can be derived from laws, norms, and contracts [1]. In addition to business processes, compliance requirements can also place demands on IT components, which in turn may be necessary for the execution of activities [2]. To satisfy compliance requirements and thus ensure compliance, so-called compliance processes can be used. A compliance process is an independent process (part) consisting of at least one compliance-related activity that ensures compliance. In addition, compliance processes can be integrated in business processes to ensure business process compliance [3].

Many factors, such as new technologies, improvement of business processes, and outsourcing decisions can lead to the replacement or removal of activities, IT components, and compliance requirements. In dynamic markets, the impact on compliance due to these changes should be determined automatically. In case of a compliance violation, the business process must also be adapted [2, 4].

There are approaches that queries the relations between compliance requirements, and business processes (e.g. [5]), compliance requirements and IT components (e.g., [6, 7]) and interrelated compliance requirements (e.g., [7]). In addition, there are also approaches that adapts the business process through the integration of separate modelled compliant process fragments (e.g., [10]). However, current approaches neither distinguish between the change patterns, replace and delete, nor do they consider IT components in both identification and adaption [8, 9].

Thus, the goal is a method to achieve compliance in flexible and IT-supported business processes. MIA supports the achievement of compliance in IT-supported business processes in two steps. On the one hand, MIA identifies the impact on compliance by removing and replacing either a compliance requirement, business activity, or IT component. On the other hand, MIA provides recommendations for a business process adaption in case of a compliance violation. In the remainder of this extended abstract, I briefly present a motivation scenario and the applied research

16th International Conference on Wirtschaftsinformatik,
March 2021, Essen, Germany

method. Then, I introduce the method MIA, its demonstration in a software prototype and evaluation, as well as possible implications and further research.

2 Motivation Scenario and Research Method

2.1 Motivation Scenario

Figure 1 shows a purchase to pay process that is supported by IT components, which are in turn connected to each other. On top of that, compliance requirements, linked together, place demands against both business activities and IT-components. The compliance process "check invoice," in turn, helps to satisfy the compliance requirement "internal policy payment." In the case of replacement or removal of an element, the impact on compliance must be determined to further achieve compliance. In case of replacing "ERP MM," which can be, e.g., the case of outsourcing, all compliance requirements that directly or indirectly place demands on this IT component must be observed. In the case of removing an element, all possible compliance violations must be determined, as well. An unplanned failure of "ERP MM" corresponds, for example, to a removal of this IT component [2].

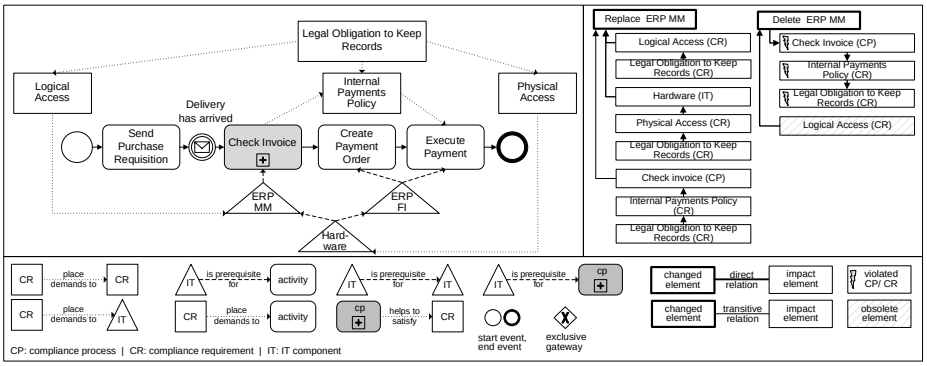


Figure 1. Purchase to pay process and impact on compliance due to a replacement and removal of an IT component [11]

2.2 Research Method

Following the design science research paradigm [12] different artifacts have been developed, which can be orchestrated to the method MIA (see Figure 2). The basis is a conceptual domain model [3], which describes the relations between compliance requirements, IT components, and business compliance processes. Essentially, MIA consists of three steps, and each of it is a separate method. First, a common model that consists of a business process model, IT components, and compliance requirements is modelled. Second, the impacts on compliance by replacing and removing any element in the previously defined common model are determined [2]. Third, to achieve business process compliance, MIA proposes recommendations for an adaption of the business

process through the integration of alternative compliance processes [4]. To distinguish compliance processes, a compliance process taxonomy was developed to describe the properties of compliance processes [3].

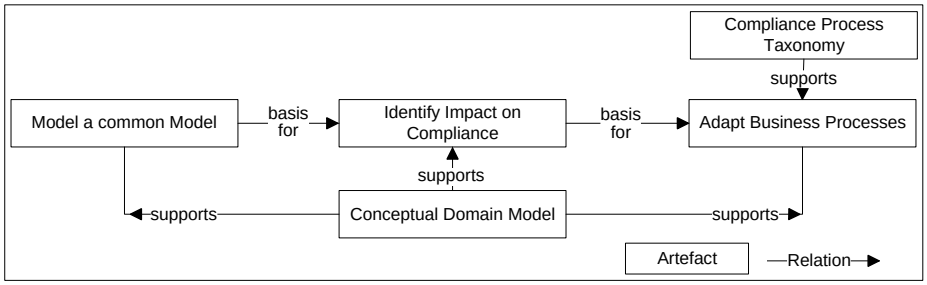


Figure 2. Artefacts of MIA

3 Achieving Compliance in Flexible and IT Supported Business Processes

3.1 A Brief Introduction to MIA

Step 1: Model a common model. To analyze the impacts on compliance when replacing and removing either a compliance requirement, business activity, and IT component, a common model, such as the one shown in Figure 1, must be modelled. These common models are based on a previously-modelled IT-architecture model (e.g., a TOGAF model), a business process model (e.g., a BPMN model) and compliance requirement model. Further, the common model is defined as a direct graph, in which each node represents either a single IT component of the IT architecture model, an event, activity, and gateway of the process model or a compliance requirement. Additionally, these nodes can be linked to each other, e.g., to define the dependency between activities and IT components, compliance requirements and activities, or different compliance requirements [2, 8].

Step 2: Identify impact on compliance. The impact on compliance due to changes differs by the type of change. In case of replacing "ERP MM" by another IT component, all compliance requirements must be determined, which affects "ERP MM" directly and transitively (see Figure 1). In case of removing "ERP MM," all violated and obsolete compliance requirements must be determined to further achieve compliance. In the motivation scenario, the compliance requirement "internal policy payment" and the higher-level compliance requirement "legal obligations to keep record" are violated because the compliance process can no longer be executed. Both analyses require different search strategies, which are executed on the common model from Step 1 [2].

Step 3: Adapt business processes. In case of a compliance violation, e.g., removing "ERP MM" as a necessary IT component of the compliance process within the business process, the business process must be adapted to remain compliant. Since more than one compliance process can satisfy a compliance requirement, a business process can be adapted through the integration of an alternative compliance process. Thus, a

prerequisite is the modelling of alternative compliance processes that satisfies the same compliance requirement. Alternative compliance processes are differentiated by their properties such as requirements for execution and type of execution [3].

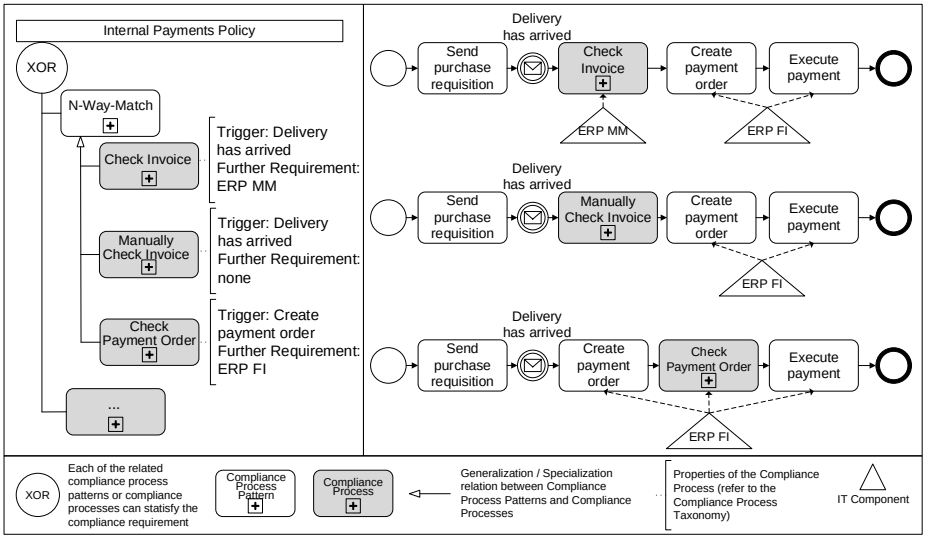


Figure 3. Adaptation of the purchase to pay process through alternative compliance processes (based on [4])

Alternative compliance processes and their related compliance requirements are modelled in a graph structure separately from the business process. Within these graph structures, the search for alternative compliance processes is completed. In case various alternative compliance processes are identified, MIA proposes all compliant business process [4] as shown in Figure 3.

3.2 Demonstration and Evaluation

To demonstrate the feasibility of MIA, we implemented the method in the software prototype BCIT [11]. BCIT allows for importing compliance requirements, business processes and IT components. Once these models are linked together, the impact by replacing or deleting any of the mentioned elements on compliance can be determined automatically. If alternative compliance processes have been defined, BCIT can also propose alternative compliant business processes through the integration of alternative compliance processes.

An addition, I evaluated the perceived usefulness of BCIT in case studies which were conducted with domain experts in the field of process management, compliance management, and IT architecture management. The data collection was done via questionnaires asking about the perceived usefulness of software artefacts. [8]. The majority of the participants find BCIT useful for their jobs. Further, they stated that BCIT gives them a greater control over their work, because of the modelling the relations between compliance requirements, business processes, and IT components.

They also mentioned that the integrated model increases the transparency of their workflow as well as the associated technical and legal dependencies. Nevertheless, some participants pointed out that the effort for both modelling of the common model and the alternative compliance processes might be too high in comparison to the expected effort.

4 Implications and Further Research

For research, there are implications to the descriptive and prescriptive knowledge bases [13]. The contribution to the descriptive knowledge base are the identified research gap, and the compliance meta- model to conceptualize our domain. The contribution to the prescriptive knowledge base includes the methods to identify compliance violations and propose compliant business process models. In addition, MIA has general implications for practice. As stated by the domain experts during the case studies, MIA opens up new potentials for detailed root cause analyses, which can result in a competitive advantage.

On the one hand, further research can be done by the process adaption. In addition to BPMN process models, formal process representations, e.g., scripting languages can also be considered. On the other hand, the idea of modelling alternative compliance processes that satisfy the same compliance requirement can also be applied to IT architectures. In this way, alternative IT components that meet the same business requirements can be modelled, e.g., in the form of different cloud service models and cloud service providers [14].

References

1. Sadiq, S., Governatori, G., Namiri, K.: Modeling Control Objectives for Business Process Compliance. In: Alonso, G., Dadam, P., Rosemann, M. (eds.) Business Process Management, 4714, pp. 149–164. Springer Berlin Heidelberg, Berlin, Heidelberg (2007)
2. Seyffarth, T., Kühnel, S., Sackmann, S.: Business Process Compliance and Business Process Change. An Approach to Analyze the Interactions. Business Information Systems. BIS 2018. Lecture Notes in Business Information Processing, 176–189 (2018)
3. Seyffarth, T., Kühnel, S., Sackmann, S.: A Taxonomy of Compliance Processes for Business Process Compliance. 15th International Conference on Business Process Management, Business Process Management Forum. In: Lecture Notes in Business Information Processing (LNBIP), 71–87 (2017)
4. Seyffarth, T., Kühnel, S., Sackmann, S.: Business Process Compliance despite Change. Towards Proposals for a Business Process Adaption. Information Systems Engineering in Responsible Information Systems. CAiSE 2019. Lecture Notes in Business Information Processing, vol 350., 227–239 (2019)
5. Fdhila, W., Rinderle-Ma, S., Knuplesch, D., Reichert, M.: Change and Compliance in Collaborative Processes. 12th IEEE International Conference on Services Computing (SCC 2015), 162–169 (2015)

6. Knackstedt, R., Eggert, M., Heddier, M., Chasin, F., Becker, J.: The Relationship Of Is And Law - The Perspective Of And Implications For IS Research. ECIS 2013 Completed Research (2013)
7. Sillaber, C., Breu, R.: Managing legal compliance through security requirements across service provider chains. A case study on the German Federal Data Protection Act. GI-Jahrestagung, 1306--1318 (2012)
8. Seyffarth, T., Kühnel, S.: Maintaining business process compliance despite changes. a decision support approach based on process adaptations. Journal of Decision Systems (2020)
9. Sackmann, S., Kühnel, S., Seyffarth, T.: Using Business Process Compliance Approaches for Compliance Management with regard to Digitization. Evidence from a Systematic Literature Review. International Conference on Business Process Management (BPM) (2018)
10. Kittel, K., Sackmann, S., Göser, K.: Flexibility and Compliance in Workflow Systems. The KitCom Prototype. Proceedings of the CAiSE'13 Forum at the 25th International Conference on Advanced Information Systems Engineering (CAiSE), 154–160 (2013)
11. Seyffarth, T., Raschke, K.: BCIT. A Tool to Recommend Compliant Business Processes based on Process Adaption. Proceedings of the Best Dissertation Award, Doctoral Consortium, and Demonstration & Resources Track at BPM 2020 co-located with the 18th International Conference on Business Process Management (BPM 2020), 107–111 (2020)
12. Peffers, K., Tuunanen, T., Gengler, C., Rossi, M., Hui, W., Virtanen, V., Bragge, J.: The Design Science Research Process. A Model for Producing and Presenting Information Systems Research. 1st International Conference on Design Science in Information Systems and Technology (DESRIST), 83–106 (2006)
13. Gregor, S., Hevner, A.R.: Positioning and Presenting Design Science Research for Maximum Impact. MIS Quarterly 37 (2013)
14. Seifert, M., Kühnel, S.: HySLAC. A Conceptual Model for Service Level Agreement Compliance in Hybrid Cloud Architectures. Informatik (2020)