Towards Secure Cloud-Computing in FinTechs – An Artefact for Prioritizing Information Security Measures

Daniel Leuthe
Research Center FIM, University of Applied Science Augsburg
daniel.leuthe@fim-rc.de

Florian Weiß
Branch Business & Information Systems Engineering of the Fraunhofer FIT
florian.weiss@fim-rc.de

Julian Dersch
University of Augsburg
julian@jdersch.com

Michael Bitzer
Research Center FIM, University of Applied Science Augsburg
michael.bitzer@fim-rc.de

Abstract

The number of FinTechs has been proliferating over the last decades. While their innovative offerings inherit disruptive potential, the security of their cloud services remains a fundamental issue. Tight budgets and the need for rapid product development force FinTechs to focus on the most necessary information security measures (ISMs) that ensure regulatory compliance and avoid customer losses due to security incidents. The question arises of how FinTechs should prioritize ISMs. To answer this question, we follow design science research to develop an artifact by which cloud service using and providing FinTechs can obtain a prioritized list of ISMs. Our resulting artifact builds upon extant research on FinTechs and information security (IS), relevant regulatory frameworks, and the shared responsibility model for cloud services. Our research contributes to the conceptualization of integrated ISM prioritization for FinTechs and provides practitioners with a structured prioritization approach based on a standardized logic.

Keywords: FinTech, Cloud Computing, Information Security, Shared Responsibility Model, Regulation

1. Introduction

Global investments in FinTech have increased more than eight-fold, from $18.9 billion in 2013 to $164.1 billion in 2022 (Pollari & Ruddenklau, 2023). FinTechs use innovative digital technologies, e.g., cloud computing (Ali et al., 2020; Fong et al., 2021), to address important unsatisfied consumer expectations, leading to their disruptive potential (Alt et al., 2018; Dorfleitner et al., 2017; Gimpel et al., 2018; Goldstein et al., 2019). Due to the competitive business environment (Chuen & Teo, 2015; Gimpel et al., 2018; Werth et al., 2023), FinTechs are forced to develop their products in a fast way (Murinde et al., 2022). Therefore, cloud computing has become a key technology for the provision of FinTech services (Werth et al., 2023). Especially the cloud's ability to i.a., allow for flexible on-demand IT resources requiring mostly utility-based operational expenditures instead of capital expenditures, led the cloud to become a fundamental part of the FinTech industry, thus constitutive for its disruptive potential (Mell & Grance, 2011; Schneider & Sunyaev, 2015; Tchernykh et al., 2019). However, due to limited resources and the opportunity-driven development, FinTechs are vulnerable to information security incidents and violations of regulation (Gai et al., 2017; Goldstein et al., 2019). Hence, their approach to leveraging cloud services represents a significant risk in becoming reliable, trustworthy, and profitable players (Mahalle et al., 2018).

Customer trust and information security (IS) are crucial success factors for FinTechs (Mehrban et al., 2020). Werth et al. (2023) describe IS as one of the most relevant objections to cloud computing within FinTechs and hence FinTech´s success. Although the operation of computing resources is sourced out to the cloud, the security responsibility is not completely transferred, but rather shared between providers and users (Armbrust et al., 2010; Mahalle et al., 2018). Those objections and the division of responsibility makes IS management even more important for FinTechs.

So far, FinTechs often tend to deprioritize IS and the compliance of certain regulations, or their prioritization lacks sophisticated approaches (Gai et al., 2017; Haupert et al., 2017). The resulting risks can lead to regulatory issues, including financial penalties, or have significant adverse effects on revenues due to declining customers' trust (Mahalle et al., 2018). Current literature identifies different clusters of information security measures (ISMs) for FinTechs, with a focus on safeguarding data, regulatory compliance, cryptography, responsibility-based access control, and secure application logic (Gai et al., 2017; Kaur et al., 2021; Singh et al., 2021). They highlight the influence of the cloud service model on IS (Mahalle et al., 2018).

Prior research has mainly addressed the provision of appropriate ISMs for FinTechs, whereas research on the prioritization of those ISMs remains scarce. Hence, FinTechs lack a comprehensive approach where to start with the implementation of which ISMs to ensure a sufficient level of both security and regulatory compliance. Thus, we raise the following research question: *How should FinTechs prioritize information security measures for cloud services?*

To address our research question, we follow the Design Science Research (DSR) paradigm (Gregor & Hevner, 2013). Based on both FinTechs-specific and empirically evaluated design objectives, we develop and

URI: https://hdl.handle.net/10125/106933
978-0-9981331-7-1

apply a FinTech cloud security measure prioritization (FCSMP) artifact. To demonstrate the artifact, we instantiate the FCSMP for FinTechs based in Germany and hence include the relevant local regulations. The FCSMP supports FinTechs in identifying and prioritizing relevant ISMs by generating an individualized list of ISMs to ensure the security of their cloud services. As will be presented later, these individual prioritized lists consider a FinTech's business type, relevant regulation, and the cloud service model. In other words, the FCSMP prioritizes ISMs based on individual FinTech-specific input variables and relevant IS factors through a standardized scoring system.

The remainder of this paper is structured as follows: In Section 2, we provide background information regarding FinTechs and cloud security. Section 3 outlines our research method. In Section 4, we present the FCSMP. Subsequently, we elucidate the instantiation and application in Section 5. Section 6 evaluates the FCSMP, including its application based on expert interviews, before we discuss our findings in Section 7 and provide a conclusion in Section 8.

2. Domain Background

2.1. FinTechs and Types of FinTechs

FinTechs offer disruptive services, products, and business models with the help of digital technologies. (Gimpel et al., 2018; Werth et al., 2023). While FinTechs share specific characteristics, e.g., leveraging digital technologies or personalized financial services, they can be clustered regarding the characteristics of their business operations (Beinke et al., 2018; Gimpel et al., 2018; Gulamhuseinwala & Kotecha, 2016; Haddad & Hornuf, 2019). The type of FinTech can impact IS requirements and potentially result in a different prioritization of an ISM. Therefore, we cluster FinTechs into six business types according to Beinke et al. (2018), Gimpel et al. (2018), Gulamhuseinwala and Kotecha (2016), and Haddad and Hornuf (2019), whereas in "other" we cluster business models that cannot be assigned to any cluster (e.g., loyalty programs):

- Banking and payment
- Trading and investments
- Financing
- Technology
- Other

2.2. Cloud Computing and Information Security within FinTechs

This paper focuses on cloud computing using or providing FinTechs. The National Institute of Standards and Technology (NIST) defines cloud computing as a technology that enables ubiquitous, convenient, and on-demand network access to a shared pool of configurable computing resources that can be provisioned with minimal management effort or interaction with the service provider (Mell & Grance, 2011). Cloud-based service models can be distinguished in software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) (Mohammed & Zeebaree, 2021). Based on the service models, control for IS lie with the customer, the provider, or both (Lane et al., 2017; Mohammed & Zeebaree, 2021). ISMs must be analyzed to determine whether one party implements them or both together, depending on the service model. Thus, both parties now split or share the responsibilities in providing adequate ISMs to the cloud system, which is defined as the shared responsibility model (Liu et al., 2011). Kaur et al. (2021) introduce an IS governance framework for FinTechs, focusing on responsibilities depending on the cloud service model.

The literature and legal frameworks, such as privacy laws and regulations, provide various definitions of IS (Bitzer et al., 2021; Solms & van Niekerk, 2013). In this regard, most definitions have the protection of the three security goals, confidentiality, integrity, and availability, in common, which we adopt in this paper (Tchernykh et al., 2019). Thus, the shared or split ISMs based on the shared responsibility model protect the three security goals of the FinTech's cloud system.

3. Method

To develop an applicable artifact, we followed the DSR paradigm (Gregor & Hevner, 2013). For structuring our research, we use the DSR process of Sonnenberg and vom Brocke (2012).

In the first step, the *Problem Identification & Motivation*, we identified the problem of FinTechs regarding the prioritization of ISMs, as discussed in Section 1. Due to limited budget and resources, the competitive business environment, and the opportunity-driven development of their services, FinTechs are forced to develop their offerings quickly, leading FinTechs to focus on the most necessary ISMs (Chuen & Teo, 2015; Gimpel et al., 2018; Murinde et al., 2022). In Step 2, *Definition of Design Objectives*, we defined the most critical influencing factors for prioritizing ISMs. Based on a literature review, our domain knowledge of working with FinTechs, and the domain-specific background (Section 2), we derived seven design objectives (DOs) focusing on IS for cloud services used and provided by FinTechs (Table 1). Due to our research question, we considered existing literature on FinTechs, cloud technology, relevant regulation, and IS regarding financial service providers.

Table 1. Derived design objectives

#	Design objective
DO1	Prioritized list of ISMs
DO2	Complete view on IS topics
DO3	FinTech type-specific prioritization
DO4	Consideration of region-specific regulatory
DO5	Consideration of FinTech-specific regulatory
DO6	Consideration of FinTech-specific importance of regulatory
DO7	Consideration of the shared responsibility model within cloud service
DO8	Necessity of an input mask and automatic generation of the result for the FinTech

According to Sonnenberg and vom Brocke (2012), we evaluated our problem definition and DOs with the aid of semi-structured expert interviews with a duration of 45 to 58 minutes each. Due to the topic's specificity, we identified the interview partners (IPs) based on our professional relations. The IPs are all based in Germany and work together with German FinTechs. Each IP belongs to a different company and guarantees extensive experience with FinTechs and IS (Table 2).

Table 2. Interview partner

IP	Role	Company affiliation	Business field
1	Compliance and Data Protection Officer	24 months	Insurance (Broker)
2	Chief Technology Officer	16 months	Banking and Payment, Technology
4	Senior Consultant	14 months	Consulting
3	Managing Partner	36 months	Consulting

Within the interviews, we discussed the challenges of FinTechs regarding the prioritization and implementation of ISMs following a predefined interview guideline. Our IPs confirmed understaffing, limited resources, strict regulatory requirements, as well as a competitive market, and a missing overview of IS topics, including the shared responsibility model, as significant challenges of FinTechs. Additionally, we discussed influencing factors regarding prioritizing ISMs. Our IPs confirmed our problem definition and acknowledged our DOs. Considering the input of the IPs, we added DO8 (Table 1). We developed the artifact during Step 3 (*Design Development)* based on the DOs and the domain background (Section 2). The artifact consists of three main input streams, first developed independently, and integrated afterwards, to generate a prioritized list of ISMs. Since FinTechs are subject to regional regulations (DO4), we first developed the input stream based on regulations. Since the applicable regulations highly depend on the business type of a FinTech, we included the type of FinTech into this first input stream (DO5). Additionally, the relevance of certain regulations can be weighted through specific input variables (DO6). We call it the *Regulatory Stream*. To account for the current security environment of FinTechs regarding the ISMs and threats, we developed the second input stream (DO2). We call it the *Threat Importance Stream*. We build upon the shared responsibility model to integrate the underlying responsibility based on the cloud service model (DO7) (Lane et al., 2017; Mell & Grance, 2011). Thus, we developed an input stream considering the used and provided shared responsibility model of the FinTech. We call it the *Shared Responsibility Stream*.

In the last step, we integrated this stream into the results of the two previous integrated streams to increase or decrease the relevance of a specific ISM depending on the shared responsibility model. We ensure an artifact that provides a FinTech-specific prioritization list (DO1, DO3) based on the previous steps.

As a last step, we transfer our artifact into a tool with an input mask and code the calculation logic so that FinTechs can receive an automatically generated result for the prioritization of relevant measures (DO8). We provide the details about the artifact and the calculation logic for the prioritization score within Section 4.

In Step 4 (*Demonstration)*, we instantiate the artifact with a set of exemplary measures. Therefore, we conducted a structured literature review in Ebsco Host, ProQuest, and IEEE Xplore. We searched for IS, cloud, and challenges in title, abstract, and keywords, starting from the year 2018 (e.g., Ebsco Host search string: *(((AB Information OR TI Information OR SU Information) AND (AB Security OR TI Security OR SU Security)) AND (AB Cloud OR TI Cloud OR SU Cloud) AND (AB Challenges OR TI Challenges OR SU Challenges)) AND (DT > 20180101)*). Our search resulted in 116 papers. We reviewed the paper's abstracts regarding their contribution to IS for cloud environments. We excluded all papers limited to only one ISM or threat and focused on those dealing with multiple measures. This resulted in 16 relevant papers for which we performed a full-text review according to the previously described criteria and a forward- and backward search of those, resulting in a final number of 12 papers. From those, we extracted 82 topics regarding IS for FinTechs using cloud services, focusing on ISMs, threats, and the associated protection goals (i.e., availability, integrity, confidentiality), where we have defined two ISMs as identical only if they have the same name in the literature. After that, we clustered these 82 topics due to their relationships in similar subject areas, resulting in 18 clusters. We identified the clusters as three information protection goals, six threats, and nine measures (Sumner, 2009). We then mapped the ISM to the threats based on the contribution to minimizing the risk of the threat. Since not all threats could be linked to measures, we conducted another more focused search on this gap and added "Planning (Infrastructure & App)"

and "HR Checks & Training", resulting in eleven ISMs. Afterward, we mapped the measures from the relevant regulatory requirements to the eleven identified measures. At this point, not all regulatory ISMs could be mapped, which is why we conducted a subsequent more in-depth search and could add five more ISMs to account for the remaining regulatory requirements. Ultimately, the resulting catalog with ISMs to cope with both IS threats and regulatory requirements encompassed 17 measures with which we instantiated the artifact (Section 5).

In Step 5, *Evaluation*, we evaluated the real-world applicability of our artifact through a prototypical implementation based on additional semi-structured interviews (Table 1). These interviews took between 90 and 120 minutes to ensure a sufficient level of detail. We describe the results of the interviews in Section 6.

4. Artefact Description

The FCSMP helps FinTechs to efficiently achieve sufficient levels of IS and regulatory compliance through the provision of individually prioritized lists with ISMs. We call the final output of the FCSMP the *Measure Priority Score* for each ISM. The higher the *Measure Priority Score*, the higher the priority to implement an ISM. As illustrated later, the *Measure Priority Score* is calculated by multiplying the *Shared Service Model Responsibility* and the *Measure Importance Score*. The *Shared Service Model Responsibility* considers if an ISM falls into the responsibility of the FinTech depending on the respective shared cloud service model (i.e., SaaS, PaaS, IaaS). Consequently, the *Measure Importance Score* considers the importance of an ISM in relation to relevant threats and protection goals (i.e., availability, integrity, confidentiality), complemented by the relevance of each ISM according to the regulations.

In the following, we present the FCSMP, its conceptual structure based on the four parts of the *Measure Priority Score* and its subparts of the *Shared Service Model Responsibility*, *Weighted Measure-Threat Importance Score*, and *Normalized Regulatory Importance Score*.

Figure 1 shows the FCSMP's structure, its calculation operators (round shapes) and computed values (square shapes), as well as the initial input variables based on the initial values from the source, e.g., literature review (square shapes shaded in blue) and the FinTech specific input values (square shapes shaded in gray). The FCSMP's input variables are in Table 3, whereby we first list the four FinTech specific input values and then the seven initial values from the source.

Table 1. Input variables for the FCSMP

Input	Description
Shared Service Model (Used)	FinTech-specific input value defines the used cloud service model (SaaS, PaaS, IaaS). For each, the value is 1 if used, 0 otherwise
Shared Service Model (Provided)	FinTech-specific input value defines the provided cloud service model. For each, the value is 1 if provided, 0 otherwise.
Type of Fintech	Indicates the business field. For each FinTech Type, one parameter is set. Hence the input consists of multiple values. Each is set to 1 if the type is applicable, 0 otherwise.
FinTech-specific Significance of Regulatory	FinTech-specific input through which the importance of regulatory can be set, whereas 0 means no relevance and 2 increased regulatory relevance.
Model-Measure Responsibility as Customer	This value is based on the shared responsibility model and derived from the input source. It determines the responsibility for a specific measure and the used service model (SaaS, Paas, IaaS). 1 means full responsibility, 0,5 partial responsibility, and 0 no responsibility. For example, for access management the values SaaS = 0,5, PaaS = 1, IaaS = 1 are set, which defines the responsibility for every possible service model used.
Model-Measure Responsibility as Provider	This value is based on the shared responsibility model and derived from the input source. It determines the responsibility for a specific ISM and the provided service model. 1 means full responsibility, 0,5 partial responsibility, and 0 no responsibility.
Protection Goal Weighting	The weighting of the three protection is defined based on the input source. This can be based on the number of mentions in the literature calculated by forming the quotient of the number of mentions of the goal and the mentions of all three goals.
Measure-Protection Goal Contribution	This parameter defines whether the ISM contributes to the specific protection goal. If the ISM affects the protection goal, the value is 1, otherwise, it is 0.
Threat Importance	This value defines a specific threat's importance according to the input source. This can be based on the number of mentions in the literature, leading to a ranking among all threats.
Number of Measures for Threat	The risk of each threat can be minimized by implementing ISMs. This parameter defines the number of ISMs related to the threat for risk minimization.
Measure Importance	This value defines a specific ISM's importance according to the input source. This can be based on the number of mentions in the literature, leading to a ranking among all ISMs.

Shared Responsibility Stream

The *Shared Service Model Responsibility* is calculated using two auxiliary variables (*Responsibility as Customer* and *Responsibility as Provider*). We calculate the auxiliary variables for each shared service model (used or provided) to determine if the FinTech is responsible for a measure. The *Responsibility as Customer* and *Responsibility as Provider* are required since FinTechs can use and provide cloud services simultaneously. For each shared service model and each ISM, the responsibility can either be 0 (no responsibility), 0.5 (shared responsibility), or 1 (full responsibility). To calculate the *Responsibility as Customer* (or the *Responsibility as Provider*), we take the maximum of all values regarding the *Responsibility for Measure*. The maximum accounts for the fact that when a FinTech uses (or provides) more than one *Shared Service Model*, always the highest responsibility for each ISM is used. To calculate the *Shared Service Model Responsibility*, we sum the *Responsibility as Customer* and the *Responsibility as Provider* for each ISM. Consequently, the *Shared Service Model Responsibility* can take the values 0, 0.5, 1, 1.5, or 2. If the FinTech is both responsible as a provider and as a customer and is fully responsible for the ISM, its *Shared Service Model Responsibility* equals 2, raising the measure's overall priority.

Threat Importance Stream

The *Weighted Measure-Threat Importance Score* is calculated through the multiplication of the *Overall Measure-Protection Goal Contribution Score* (representing the ISM's contribution to the three protection goals) and the *Measure-Threat Importance Score* (indicating the measure's importance according to threat mitigation effectiveness). The *Overall Measure-Protection Goal Contribution Score* can take values between 0 and 1 depending on which protection goals are affected by the ISM. Each affected protection goal has its own *Protection Goal Weighting* according to the initial source, whereas the sum of all three *Protection Goal Weighting*s equals 1. The weighting represents the goal's importance according to the input source. Furthermore, the binary input value *Measure Protection Goal Contribution* expresses if the protection goal is affected by the ISM (1) or not (0). The individual *Measure-Protection Goal Contribution per Protection Goal* is calculated for each protection goal by multiplying the *Protection Goal Weighting* and the *Measure Protection Goal Contribution*. The final *Overall Measure-Protection Goal Contribution Score* for each measure is then computed by summing up the individual values per protection goal. The computed *Measure-Threat Importance Score* consists of two values, the *Share of Threat Importance* and the input value *Measure Importance*, which are added up because both represent independent values. It is essential for the *Share of Threat Importance* to understand that every threat has a likelihood to cause harm and a possible impact (Bitzer et al., 2021). Both can be minimized by implementing ISMs. Thus, every threat can be related to one or more ISMs. For the calculation, the *Threat Importance*'s value has to be distributed across the respective ISMs, whereby the threat value originates from the input source, as shown in Table 3 (e.g., the number of mentions in the literature). We divide this value by the *Number of Measures for Threat*, which defines the number of ISMs related to the threat for risk minimization. The second component is the *Measure Importance* which represents the importance of a specific ISM according to the input source and can be any integer number greater than 0, which leads to a ranking among all ISMs. For example, this value can be specified through performing a structured literature review and deriving the ISM's relevance from the number of its mentions.

Regulatory Stream

The *Normalized Regulatory Importance Score* indicates the importance of each ISM according to regulation. On the one hand, it depends on the underlying *Type of FinTech* (Section 2.1). Based on the *Type of FinTech*, it is determined for each regulation if the regulation and its associated ISMs are relevant for the specific *Type of FinTech*, resulting in the *Type-specific Significance of Regulatory*. If applicable, the *Type-specific Significance of Regulatory* receives the value 1; otherwise, it is set to 0. Also, it depends on the *FinTech-specific Significance of Regulatory*. This indicates the importance of regulations from the FinTech's point of view, ranging from a value of 0 (no increased importance) to the value of 1 (increased importance) and the value of 2 (strongly increased importance). The *Type-specific Significance of Regulatory* and the *FinTech-specific Significance of Regulatory* are added up to receive the *Regulatory Importance Score* for the FinTech, resulting in a value of either 0, 1, 2, or 3. To account for the fact that the scores for measures derived from the regulatory should be comparable to those derived from literature, the *Regulatory Importance Score* is multiplied by the *Regulatory Normalization Factor (*based on the average of the *Weighted Measure-Threat Importance Score* as described), which leads to the overall *Normalized Regulatory Importance Score*. This ensures that none of the in the further calculation computed values are neither over- nor underweighted.

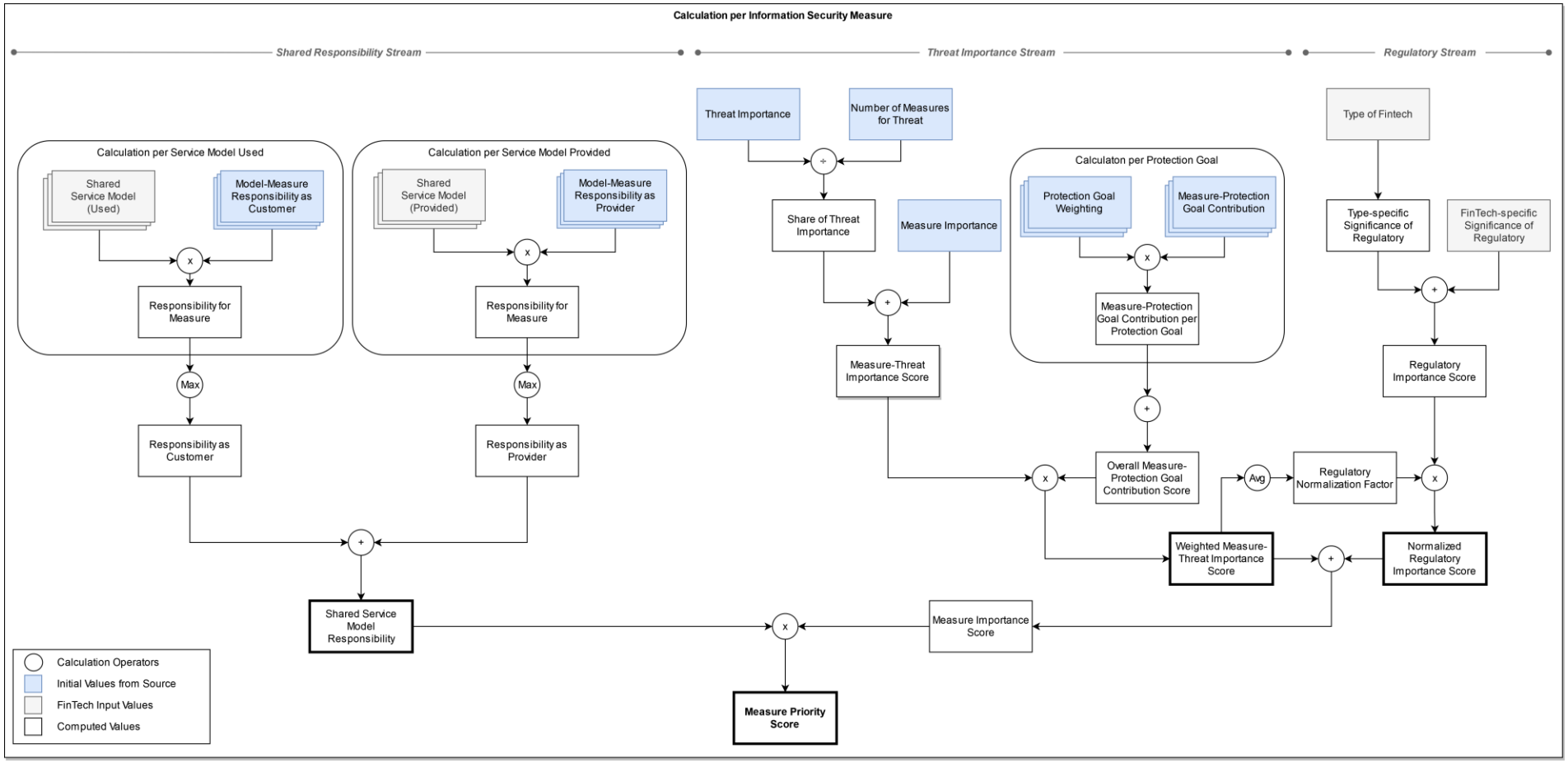

Figure 1. Structure and calculation schema of the FCSMP

5. Instantiation and Demonstration

We instantiate the FCSMP for the case of a German FinTech to demonstrate its outputs and computational logic. Hence, we consider the three following regulations of the German legislator and authorities: the Minimum Requirements for Risk Management (MaRisk), Banking Supervisory Requirements for IT (BAIT), and Insurance Supervisory Requirements for IT (VAIT). These regulations contain direct ISMs, including IT systems' development, IT governance, IS management (i.e., determination of safety representatives, incident response management, emergency management), user authorization management, application development (including end-users), data backup and operations requirements (Dorfleitner et al., 2017; Kunschke et al., 2022; Maksimovic & Biernat, 2019); (Maksimovic & Biernat, 2019). According to Kunschke et al. (2022) and Dorfleitner et al. (2017), the regulations can be mapped to the identified types of FinTechs (Table 4).

Table 2. Relevant regulation

Regulation	Relevance for Fintech type
MaRisk	Banking and payment, Trading and investments, Insurance, Financing
BAIT	Banking and payment, Trading and investments, Financing
VAIT	Insurance

To demonstrate the applicability of the FCSMP, first, we use the example of *Authorization Management* as a measure to describe how we derive its *Measure Priority Score* step by step. Second, we provide the final *Measure Priority Score* (MPS) for all remaining measures. The results are depicted in Table 5. Due to the small amount of data and the FCSMP's standardized calculation logic, we use the spreadsheet program Excel for the implementation.

Table 3. Prioritization of the ISMs

Measure	MPS
Authorization Management	43
Contractual Agreement on Shared Responsibility	26
IS Management (excl. emergency management)	25
Information Risk Management (excl. information and protection needs)	25
IT Strategy	25
IT Projects, Application Development (incl. End User Departments)	25
Communication/Network Security	20
Backups & Business Continuity Measure	19
IT Operations (excl. Data Backup)	19
Segregation of Data	14
Planning (Infrastructure & App)	13
Application Security	13
Virtualization	13
HR Checks & Training	12
APIs	11
Encryption	9
Physical Security	1

For this demonstration, we consider a FinTech belonging to the two business types of Insurance and Technology. Furthermore, the used cloud service models are IaaS and PaaS, while the provided Model is SaaS. The input values for the used and provided cloud service models are set accordingly. Moreover, the *FinTech-specific Significance of Regulatory* is of increased importance (i.e., equals 1).

The *Protection Goal Weighting* for the ISM *Authorization Management* is set to 2/16 for availability, 9/16 for confidentiality, and 5/16 for integrity based on the input source literature. Since all protection goals are affected by the considered ISM, we set the *Measure-Protection Goal Contribution* to 1 for every goal. After conducting the multiplication and adding up the *Measure-Protection Goal Contribution per Protection Goal* the result is 1. For the considered ISM only the threat "attacks against person" is relevant. Based on the preceding review of literature, the *Threat Importance* is set to 6. Also, two measures were identified to minimize the risk of this threat. Accordingly, we set the *Number of Measures for Threat* to 2. The *Share of Threat Importance* results in 3. We derive the *Measure Importance* of 13 from literature and add the *Share of Threat*. This results in a *Measure-Threat Importance Score* of 16. Subsequently, we determine a *Weighted Measure Threat Importance Score* of 16,00 by multiplying the *Measure-Protection Goal Contribution per Protection Goal* and the *Measure-Threat Importance Score*.

According to our example, the *Type of FinTech* is set to 1 for Insurance and Technology. Hence, we derive the value 1 for the *Type-specific Significance of Regulatory*. According to the example, we set the input value *FinTech-specific Significance of Regulatory* to 1 and sum it up with the *Type-specific Significance of Regulatory*, which results in the *Regulatory Importance Score* of 2. We calculate the *Regulatory Normalization Factor* by taking the average of all *Weighted Measure Threat Importance Scores* (6,20) and multiplying it with the *Regulatory Importance Score*. Ultimately, we recieve a *Normalized Regulatory Score* of 12,40.

Lastly, we compute the *Shared Service Model Responsibility*. The input value *Shared Service Model (Used)* is set to 1 for IaaS and PaaS and 0 for SaaS according to the example setting whereas the *Model-Measure Responsibility as Customer* for the service models are 1 (IaaS), 0,5 (PaaS) and 0,5 (SaaS). Thus, the *Responsibility as Customer* is set to 1. The input value *Shared Service Model (Provided)* is set to 0 for

IaaS and PaaS and 1 for SaaS according to the example setting, whereas the *Model-Measure Responsibility as Customer* for the service models are 0 (IaaS), 0,5 (PaaS), and 0,5 (SaaS). According to the assumed partial ISM implementation responsibility, the *Responsibility as Provider* equals 0,5. Consequently, the *Shared Service Model Responsibility* equals 1,5. In the last step, we multiply the sum of the *Weighted Measure Threat Importance Score* (16,00) and the *Normalized Regulatory Importance Score* (12,40) with the *Shared Service Model Responsibility* (1,5) to receive the *Measure Priority Score* for *Authorization Management* ((16,00 + 12,40) x 1,5 = 42,60). To avoid a false sense of accuracy, we round the *Measure Priority Score* to an integer value. Accordingly, the *Measure Priority Score* for *Authorization Management* is 43. In our instantiation, we determined the *Measure Priority Score* of all ISMs the same way.

6. Evaluation

Following Sonnenberg and vom Brocke (2012), we conducted an ex-post evaluation through semi-structured expert interviews, which focused on assessing the artifact's design. We performed the evaluation with the same IPs throughout the problem definition and DOs evaluation phase (Table 1). First, we discussed their views on relevant factors for prioritizing ISMs for FinTechs and compared their opinions with the prioritization factors of the FCSMP. Second, we presented the FCSMP, its calculation logic, and its prototypical implementation. Furthermore, we asked the interviewees to evaluate the fulfilment of the DOs. At any time, the interviewees could contribute their suggestions for further improvement of the FCSMP.

Overall, our IPs agreed on the input streams and their relevance for the FCSMP. They confirmed that the division of the FCSMP's input values into both FinTech-specific input values and initial input values from current IS environment (e.g., literature review as shown in the instantiation) is necessary to, on the one hand, capture the specific circumstances of the FinTech and, on the other hand, to capture current and relevant IS topics. Moreover, the FCSMP was reported to cover the most relevant influencing factors for a first simplified prioritization of ISMs for FinTechs based on a standardized calculation logic, whereas the most important aspect constitutes the influence of regulation on the prioritization of IS issues via regulatory requirements. Beyond their confirmations, however, IP1 recommended including the processed data of the FinTech and thus differentiating between the criticality of the processed data within the type of FinTech, such as the gradation of a low, medium, or high data criticality. However, it was decided to always assume the highest data criticality to keep the artifact's complexity manageable.

Based on the third part of the interviews, we evaluated the successful implementation of our DOs throughout the instantiation (Table 6).

Table 4. Implementation of the design objectives

#	Description of Fulfilment
DO1	Measures receive a score dependent on the derived threats, relevant regulatory, and the business model.
DO2	Is fulfilled through the extraction of relevant IS topics based on the literature review and regulation.
DO3	The FCSMP considers the type of FinTech for defining the relevant regulations as a FinTech-specific input value. All relevant German regulations and their measures are considered.
DO4	
DO5	
DO6	The FinTech can provide its specific importance of regulatory as an input value.
DO7	Based on two input streams, the used and provided shared service models are considered. For each measure, the responsibilities are provided as inputs.
DO8	A prototypical implementation was developed in form of an Excel-Tool. Automated ISM prioritizations based on input values are generated.

With the realization of all DOs completed, we presented our results to industry experts from an international top-tier management consultancy as part of the final step of DSR (Communication). To date, this consultancy has adopted the artifact's logic to explain its ISM identification procedures to FinTech-industry clients.

7. Discussion

The prioritization of ISMs constitutes a major issue for FinTechs. Our FCSMP accounts for the most relevant factors that FinTechs with cloud services need to consider, i.e., their business model, relevant regulatory, and their used and provided cloud model.

Regarding the extant knowledge on FinTechs, we emphasize the need for research on how to ensure IS within the cloud environment with limited resources. While literature provides multiple insights on ISMs (Gai et al., 2017; Mahalle et al., 2018; Singh et al., 2021), we go one step further and provide an artifact that consolidates existing insights and makes them actionable for FinTechs by selecting relevant ISMs and calculating their priority based on relevant input factors, present IS knowledge, and FinTech-specific inputs through a standardized calculation logic.

Additionally, we add to the important stream of IS in information systems literature (Vial, 2019; Wu et al., 2015). Although focusing on FinTechs with cloud services, we provide a structured method for quantitatively determining the priority of ISMs. Even though IS research is not a novel topic (Vial, 2019) and

established organization-wide concepts to evaluate the risk of threats exist (DIN ISO 31000; NIST), structured approaches for quantitative decision support for the prioritization of ISMs are scarce. In contrast to existing approaches, the FCSMP allows for considering state-of-the-art knowledge regarding threats, measures, regulations, and cloud services based on chosen sources (e.g., literature review). Overall, we provide researchers with a first conceptual artifact for prioritizing ISMs through a standardized, quantitative method.

For FinTechs with cloud services, we offer a structured and practical approach for prioritizing ISMs based on individual input values. Thus, we support FinTechs to efficiently allocate their resources regarding IS. While the artifact does not consider all factors, e.g., criticality of processed data, the artifact can be used as a basis for prioritization. Further, the influencing factors of the shared service model refer to established standards like NIST.

Besides the merits, our research has three limitations. First, our artifact simplifies the totality of all influencing factors and their interrelations. While we propose that simplification is a major benefit for decision-making, we also acknowledge that there is no one-size-fits-it-all approach. The FCSMP does not consider a FinTech's strategic orientation, its size, the type of processed data, or interdependencies between ISMs. Thus, practitioners should use the artifact mindfully and extend it on a detailed level with expert knowledge. Further, this limitation provides opportunities for research to extend our artifact based on identified shortcomings within the instantiation. Second, the instantiation delivers a snapshot that needs to be continuously revised. Accordingly, the instantiation is limited to time (snapshot) and context (regionally and industry-specific regulations). For example, on the one hand, our instantiation is limited to 17 exemplary ISMs based on a comprehensive literature review. Hence, the relevance of individual ISMs depend on the completeness of IS literature. On the other hand, our instantiation focuses on German regulatory. While the context, i.e., nationally applicable regulations and the type of FinTech, will always need to be considered, and the undertaken instantiation may take a lot of effort for small-sized FinTechs with limited resources, future research might find promising ways to calculate the *Measure Priority Score* in a timely and automatized way and to improve the research's generalizability. Third, we evaluated the problem definition, the DOs, and our FCSMP based on semi-structured expert interviews. We acknowledge, on the one hand, that we conducted the three parts with the same four experts and, on the other hand, the limitations of interviews as an evaluation method. However, we consider four interviews as a minimal number for evaluation since the analysis of the FCSMP revealed consistent insights across a heterogeneous group regarding the area of expertise. Nevertheless, the evaluation is limited to an exemplary FinTech, and we claim that a real-world application should be conducted.

8. Conclusion

This paper addresses the relevant issue of IS in FinTechs. In response to the current lack of a practical approach that helps FinTechs to prioritize ISMs to achieve sufficient levels of IS, we developed an artifact to support this process. For calculating the priority of an ISM, our artifact considers relevant factors, e.g., relevant regulations, threats, protection goals, as well as the FinTech's business model. We consulted experts from practice to ensure both viability and real-world applicability, which helped us to derive DOs and evaluate the artifact. We encourage IS researchers to challenge and extend the artifact to further areas of application and incorporate additional relevant factors for the prioritization of ISMs.

9. References

Ali, O., Shrestha, A., Chatfield, A., & Murray, P. (2020). Assessing information security risks in the cloud: A case study of Australian local government authorities. *Government Information Quarterly*, *37*(1), 101419.

Alt, R., Beck, R., & Smits, M. T. (2018). FinTech and the transformation of the financial industry. *Electronic Markets*, *28*(3), 235–243. https://doi.org/10.1007/s12525-018-0310-9

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM*, *53*(4), 50–58. https://doi.org/10.1145/1721654.1721672

Beinke, J. H., Nguyen, D., & Teuteberg, F. (2018). Towards a business model taxonomy of startups in the finance sector using blockchain. *ICIS 2018*.

Bitzer, M., Brinz, N., & Ollig, P. (2021). Disentangling the Concept of Information Security Properties: Enabling Effective Information Security Governance. *ECIS 2021*.

Chuen, D. L. K., & Teo, E. G. S. (2015). Emergence of fintech and the LASIC principles. *The Journal of Financial Perspectives: Fintech*, 24–37.

Dorfleitner, G., Hornuf, L., Schmitt, M., & Weber, M. (2017). The fintech market in Germany. In *FinTech in Germany* (pp. 13–46). Springer.

Fong, D., Han, F., Liu, L., Qu, J., & Shek, A. (2021). *Seven technologies shaping the future of fintech*. https://www.mckinsey.com/cn/our-insights/seven-technologies-shaping-the-future-of-fintech

Gai, K., Qiu, M., Sun, X., & Zhao, H. (2017). Security and Privacy Issues: A Survey on FinTech. In M. Qiu (Ed.), *Lecture Notes in Computer Science: Vol. 10135. Smart computing and communication: First international conference, SmartCom 2016* (Vol. 10135, pp. 236–247). https://doi.org/10.1007/978-3-319-52015-5_24

Gimpel, H., Rau, D., & Röglinger, M. (2018). Understanding FinTech start-ups–a taxonomy of consumer-oriented service offerings. *Electronic Markets*, *28*(3), 245–264.

Goldstein, I., Jiang, W., & Karolyi, G. A. (2019). To FinTech and Beyond. *The Review of Financial Studies*, *32*(5), 1647–1661. https://doi.org/10.1093/rfs/hhz025

Gregor, S., & Hevner, A. R. (2013). Positioning and presenting design science research for maximum impact. *MIS Quarterly*(37), Article 2, 337–355.

Gulamhuseinwala, I., & Kotecha, V. (2016). *UK FinTech on the cutting edge: An evaluation of the international FinTech sector*. https://www.gov.uk/government/publications/uk-fintech-on-the-cutting-edge

Haddad, C., & Hornuf, L. (2019). The emergence of the global fintech market: economic and technological determinants. *Small Business Economics*, *53*(1), 81–105. https://doi.org/10.1007/s11187-018-9991-x

Haupert, V., Maier, D., & Müller, T. (2017). Paying the Price for Disruption. In *Proceedings of the 1st Reversing and Offensive-oriented Trends Symposium.* ACM. https://doi.org/10.1145/3150376.3150383

Kaur, G., Habibi Lashkari, Z., & Habibi Lashkari, A. (2021). Information Security Governance in FinTech. In G. Kaur, Z. Habibi Lashkari, & A. Habibi Lashkari (Eds.), *Understanding Cybersecurity Management in FinTech* (pp. 35–64). Springer International Publishing. https://doi.org/10.1007/978-3-030-79915-1_3

Kunschke, D., Spitz, M. F., & Pohle, J. (2022). *FinTech*. Erich Schmidt Verlag GmbH & Co. KG. https://doi.org/10.37307/b.978-3-503-20689-6

Lane, M., Shrestha, A., & Ali, O. (2017). Managing the risks of data security and privacy in the cloud: a shared responsibility between the cloud service provider and the client organisation. *Bright Internet Global Summit*.

Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., & Leaf, D. (2011). *NIST cloud computing reference architecture.* https://doi.org/10.6028/NIST.SP.500-292

Mahalle, A., Yong, J., Tao, X., & Shen, J. (2018). Data Privacy and System Security for Banking and Financial Services Industry based on Cloud Computing Infrastructure. In W. Shen, J. Luo, J.-P. Barthès, F. Dong, J. Zhang, & H. Zhu (Chairs), *2018 IEEE 22nd International Conference on Computer Supported Cooperative Work in Design (CSCWD)*.

Maksimovic, T., & Biernat, H. (2019). MaRisk und BAIT im Detail. In T. Maksimovic & H. Biernat (Eds.), *Bankaufsichtliche Anforderungen an die IT.* Springer Gabler. https://doi.org/10.1007/978-3-658-25226-7_2

Mehrban, S., Khan, M. A., Nadeem, M. W., Hussain, M., Ahmed, M. M., Hakeem, O., Saqib, S., Kiah, M. L. M., Abbas, F., & Hassan, M. (2020). Towards Secure FinTech: A Survey, Taxonomy, and Open Research Challenges. *IEEE Access*, *8*, 23391–23406. https://doi.org/10.1109/ACCESS.2020.2970430

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. *Computer Security Resource Center*.

Mohammed, C. M., & Zeebaree, S. R. M. (2021). Sufficient Comparison Among Cloud Computing Services: IaaS, PaaS, and SaaS: A Review. *International Journal of Science and Business.* Advance online publication. https://doi.org/10.5281/ZENODO.4481415

Murinde, V., Rizopoulos, E., & Zachariadis, M. (2022). The impact of the FinTech revolution on the future of banking: Opportunities and risks. *International Review of Financial Analysis*, 102103. https://doi.org/10.1016/j.irfa.2022.102103

Pollari, I., & Ruddenklau, A. (2023). *The Pulse of Fintech 2022: Global analysis of fintech investment*. https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2023/02/pulse-of-fintech-h2-22-web-file.pdf

Schneider, S., & Sunyaev, A. (2015). CloudLive: a life cycle framework for cloud services. *Electronic Markets*, *25*(4), 299–311.

Singh, G., Gupta, R., & Vatsa, V. (2021, October 11 – December 11). A Framework for Enhancing Cyber Security in Fintech Applications in India. In *2021 International Conference on Technological Advancements and Innovations* (pp. 274–279). IEEE. https://doi.org/10.1109/ICTAI53825.2021.9673277

Solms, R. von, & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Sonnenberg, C., & vom Brocke, J. (2012). Evaluations in the Science of the Artificial – Reconsidering the Build-Evaluate Pattern in Design Science Research. In *Design Science Research in Information Systems. Advances in Theory and Practice* (Vol. 7286, pp. 381–397). https://doi.org/10.1007/978-3-642-29863-9_28

Sumner, M. (2009). Information security threats: a comparative analysis of impact, probability, and preparedness. *Information Systems Management*, *26*(1).

Tchernykh, A., Schwiegelsohn, U., Talbi, E., & Babenko, M. (2019). Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability. *Journal of Computational Science*, *36*, 100581. https://doi.org/10.1016/j.jocs.2016.11.011

Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems*, *28*(2), 118–144. https://doi.org/10.1016/j.jsis.2019.01.003

Werth, O., Cardona, D. R., Torno, A., Breitner, M. H., & Muntermann, J. (2023). What determines FinTech success?-A taxonomy-based analysis of FinTech success factors. *Electronic Markets*, *33*(1), 21. https://doi.org/10.1007/s12525-023-00626-7

Wu, S. P.-J., Straub, D. W., & Liang, T.-P. (2015). How Information Technology Governance Mechanisms and Strategic Alignment Influence Organizational Performance: Insights from a Matched Survey of Business and IT Managers. *MIS Quarterly*, *39*(2), 497–518. https://doi.org/10.25300/MISQ/2015/39.2.10