2024

A Literature-Driven Design Theory for Multiple-Criteria Assessment Tools for Information Security Investments

Laura Bauer
Martin Luther University Halle-Wittenberg, laura.bauer@wiwi.uni-halle.de

A Literature-Driven Design Theory for Multiple-Criteria Assessment Tools for Information Security Investments

Research Paper

Laura Bauer

Martin Luther University Halle-Wittenberg, Chair for Business Information Management, Halle (Saale), Germany
laura.bauer@wiwi.uni-halle.de

Abstract. The growing number of security threats nowadays and the substantial economic losses they cause have increased the importance of information security for companies worldwide. Regarding a company's information security investments, it is therefore crucial to ensure its adequate protection and at the same time act economically efficient. Assessment tools can support the selection of economically efficient information security investments. However, most assessment tools focus on monetary criteria and ignore the large number of relevant non-monetary criteria. Hence, there is a need for guidance to develop multiple-criteria assessment tools. As existing frameworks do not address this need, this study presents design requirements and design principles for the development of multiple-criteria assessment tools for information security investments. The proposed design theory provides fundamental design knowledge and offers guidance to build comprehensive assessment tools.

Keywords: Information Security, Multiple-Criteria Assessment, Design Theory.

1 Introduction

Companies today are strongly connected within their own organizational structure as well as with other companies (Balozian et al. 2023, Jiang et al. 2023). The tightening information security (InfoSec) situation, with a growing number of security threats in the past years, is affecting companies even more and causes serious economic losses (Dhillon et al. 2020, Weishäupl et al. 2015b). In Germany, the damage induced by cybercrime in 2023 was estimated at a total of 205.9 billion euros (Statista 2024). This included tangible costs, such as damage to information technology (IT), as well as intangible costs, such as reputational damage (Statista 2024). The prioritization of InfoSec and the protection of a company's processes, data, and technologies is therefore essential for a company's economic success (Guggenmos et al. 2022, Kühnel et al. 2021, Weishäupl et al. 2015a). Thus, companies use large parts of their IT budget for InfoSec investments, sometimes even running the risk of over-investing (Li et al. 2019, Srinidhi et al. 2015). A company's objective should, however, be to conduct InfoSec

19th International Conference on Wirtschaftsinformatik,
September 2024, Würzburg, Germany

investments most effectively (Bodin et al. 2005, Jiang et al. 2023). Those include investments in "technology, processes, and people" (Zafar & Clark 2009, p. 572).

As a solid foundation of such investment decisions, assessment tools for InfoSec investments, presented as information systems (IS) by Schatz and Bashroush (2017), offer guidance to systematically assess and prioritize investments (Bodin et al. 2005, Dor & Elovici 2016). In literature, qualitative and non-monetary criteria for such assessments relating to, among other things, behavioral aspects of a company are often given less consideration (Heidt et al. 2019). There is a greater focus on the consideration of monetary criteria (Heidt et al. 2019). However, the significance of these assessment tools depends on the information available to the user (Ebbers et al. 2021, Mithas et al. 2013, Wanner et al. 2020). Yet, this necessary information often cannot be provided as not all criteria for a comprehensive assessment of InfoSec investments can be presented in monetary terms. (Shao et al. 2020). Hence, purely monetary assessment tools do not present a satisfactory solution for assessments of InfoSec investments. InfoSec experts should rather consider multiple criteria when assessing the investment in security measures, instead of focusing on traditional financial metrics, such as costs and benefits (Kuehnel et al. 2019, Shao et al. 2020, van Looy & Shafagatova 2016).

As the development of assessment tools for InfoSec investments is challenging, a few approaches in literature already exist (e.g., Matschak et al. 2023, Mujinga et al. 2017). Yet, to the best of my knowledge, a generally applicable design theory (DT) with specific design requirements (DRs) or DPs that supports the development of multiple-criteria assessment tools for InfoSec investments does not exist. Therefore, the following research question (RQ) is raised:

What are design requirements and design principles for the development of a multiple-criteria assessment tool for information security investments?

To answer the research question, I provide a set of DRs and DPs by applying the method for DP development of Möller et al. (2020). In this study, the method is based on a systematic literature review (SLR) following vom Brocke et al. (2009). The DT shall offer support for academia and practice in the development of new multiple-criteria assessment tools and specific software artifacts.

The paper is structured as follows, Chapter 2 briefly discusses the theoretical background. Chapter 3 describes the methodology of the study. Chapter 4 presents the results and Chapter 5 presents their evaluation. In Chapter 6 the theoretical and practical implications of this study as well as the limitations and future research directions are discussed. Chapter 7 concludes the paper.

2 Theoretical Background

The analysis of economically reasonable InfoSec investments and the efficient implementation of security measures have been part of academic literature for some time now (Jiang et al. 2023, Li et al. 2019, Weishäupl et al. 2015a). In most studies, a differentiation is made between two dominant research streams, game theory and risk and return approaches (Niedzela et al. 2023, Shao et al. 2019, Weishäupl et al. 2015a). Concerning these, researchers (e.g., Ebbers et al. 2021, Heidt et al. 2019, Schatz &

Bashroush 2017) criticize the one-dimensionality of such approaches, as they mostly ignore an organization's application context. This might lead to the neglect of relevant assessment criteria and poor assessment results (Niedzela et al. 2022). One known example is the approach of the return on security investment (ROSI). It is frequently applied in current literature (e.g., Shao et al. 2020, Weishäupl et al. 2018).

Accordingly, among others, Llansó et al. (2019) and van Looy & Shafagatova (2016) emphasize the value of a multiple-criteria assessment of InfoSec investments which causes balanced investment decisions adapted to a company's context. Multiple-criteria approaches integrate the aspect of multidimensionality in their assessments (Chen et al. 2013, Huang & Huang 2014). Such approaches, therefore, do not focus on monetary criteria, such as 'implementation costs', but also apply numerous non-monetary criteria, such as a 'company's reputation', 'service quality', or 'process flexibility' (Kühnel et al. 2021, Llansó et al. 2019). These non-monetary and qualitative criteria are strongly important for the performance of a company and therefore influence its profitability (Kühnel et al. 2021). For their assessment, however, commonly expert knowledge has to be used, resulting in information with a at least partly subjective character (Sheen 2010). Yet, multiple-criteria approaches still provide a comprehensive view of the assessment problem (Huang & Huang 2014, Kühnel et al. 2021).

In InfoSec literature, some approaches for InfoSec investments have already been discussed. Matschak et al. (2023) identify specific functional requirements for the development of an IT tool for InfoSec investment assessments with a focus on the health and energy sector. Mujinga et al. (2017) develop a design framework of design principles (DPs) for InfoSec tools and consider social as well as technical aspects in their study. Additionally, in relation to the implementation of such tools, some literature exists that discusses aspects of potential barriers to the implementation of InfoSec assessment tools or factors that could promote their acceptance (e.g., Bandyopadhyay & Zafar 2017, Heidt et al. 2019, Niedzela et al. 2023, Vedadi et al. 2021).

3 Methodology

The goal of this design science research (DSR) project is to develop a DT (Möller et al. 2020) for multiple-criteria assessment tools of InfoSec investments. The foundation of a DT consists of DRs and DPs, which offer a design solution for a previously defined problem and thus support the development of an information system (IS) (Walls et al. 1992). While DRs describe subordinated goals and objectives for a class of IS (Baskerville & Pries-Heje 2010, Walls et al. 1992), DPs, which refer to the DRs, provide solution principles that offer guidance for the design process (Fu et al. 2016).

For the development of the DT, the method of Möller et al. (2020) was applied consisting of seven steps. In this paper, the results of a complete iteration of Möller et al.'s (2020) method are presented (see Table 1). After formulating the solution objective (step I) and specifying the research context within DSR (step II), the supportive approach of Möller et al. (2020) was chosen (step III), since the DT should not draw on a specific software artifact. Here, the DT is developed before the instantiation of an IS.

Table 1. Methodical Steps following Möller et al. (2020)

Methodical Steps		Instantiation
I	Formulate Solution Objective	***What are design requirements and design principles for the development of a multiple-criteria assessment tool for information security investments?***
II	Specify Research Context	***Design Science Research*** for the development of a comprehensive design theory consisting of design requirements and design principles for assessment approaches for information security investments.
III	Select Research Approach	***Supportive-Approach*** to provide design knowledge for specific IT artifacts of assessment approaches of InfoSec investments (ex-ante).
IV	Identify Knowledge Base	***Systematic literature review*** to derive design requirements and to derive design principles responding to the design requirements.
V	Elicit Meta Requirements	***4 design requirements*** from 28 relevant papers
VI	Formulate Design Principles	***11 design principles*** from 28 relevant papers and in response to the design requirements
VII	Evaluate	***Moderated focus group***

As a knowledge base, an SLR following the rigorous procedure of vom Brocke et al. (2009) was conducted (step IV). Therefore, I started in the introduction by putting the research into context, followed by the definition of the research scope, the description of the literature search process, and the analysis of the final literature. For the definition of the research scope, the six characteristics of Cooper's (1988) "Taxonomy of Literature Reviews" were applied. The (1) focus was on research outcomes and theories with a (2) goal to synthesize key findings. The (3) perspective was neutral. The (4) coverage was exhaustive with selective criticism, and the (5) organization of the results was conceptual. Lastly, with this study, an (6) audience of specialized scholars and practitioners is addressed. For the literature search process (see Figure 1), a title, abstract, and full-text search was applied by using a previously defined search string.

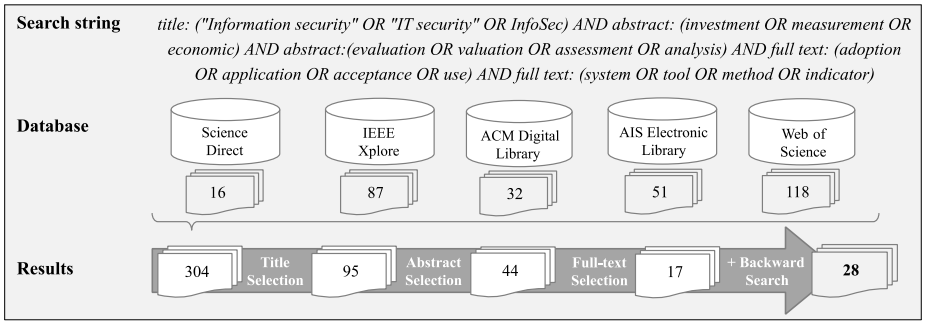

Figure 1. Literature Search Process

To find articles that suit this research best, selection criteria were defined following Kitchenham et al. (2009). The literature review consisted of a title selection, abstract selection, full-text selection, and a backward search. Figure 1 illustrates the number of articles identified at each stage and ultimately used to develop the DT. The findings drawn from the finally identified literature were formulated as DRs and DPs according

to Fu et al. (2016) (steps V and VI). In doing so, it was made sure that the DPs refer to the previously formulated DRs. Once the DT was formed, it was presented and evaluated within a moderated focus group (MFG) following Morgan (1997) (step VII) using evaluation criteria of Gregor and Hevner (2013) and Iivari et al. (2021).

4 Results

The final design theory of this study can be seen in Figure 2. The 4 DRs and 11 DPs from the final 28 papers identified in the SLR are described below. For reasons of readability, not all papers referencing a DR and DP are mentioned in the description of it. For the specific assignment of the identified publications to the individual concepts, on the level of DPs, see Table 2 in this paper's appendix.

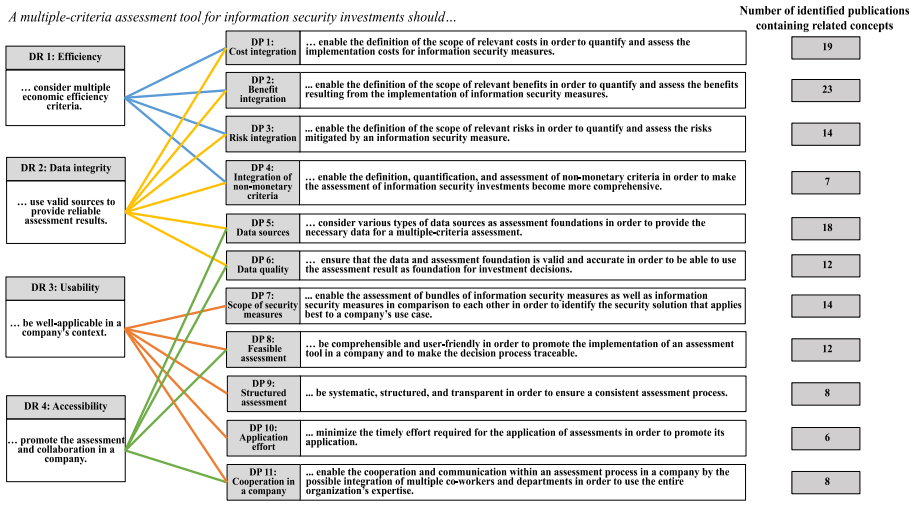

Figure 2. Design Theory

Multiple-criteria assessment tools for InfoSec investments should focus on the accomplishment of their global goal (Schatz & Bashroush 2017). They assess InfoSec investments by financial efficiency criteria, such as investment costs and benefits (Schatz & Bashroush 2017). Considering an investment's benefit, this could be compared to a company's InfoSec budget as well as the InfoSec risks (Fielder et al. 2016, Neubauer & Hartl 2009). Thereby, a prioritization of different investment options could be conducted (Buck & Hanf 2008). In addition, multiple-criteria assessment tools are deemed to be economically efficient if they also include non-monetary criteria that strongly influence the profitability of an investment (Bodin et al. 2005). Such non-monetary criteria, especially in combination with monetary criteria, reflect the real-world complexity of investment decisions (Schilling & Werners 2015). Therefore, I

propose **DR 1: "Efficiency":** *A multiple-criteria assessment tool for information security investments should consider multiple economic efficiency criteria.*

Multiple-criteria assessment tools aim to use valid data (Schilling & Werners 2015). The data demand should thereby be compatible with a company's data supply (Bojanc & Jerman-Blažič 2008b). Via an integration of recorded historical data (Schatz & Bashroush 2017) as well as subjective data based on an individual experience and expertise (Weishäupl et al. 2018), a multitude of valid data are generated. Therefore, valuable information for a comprehensive assessment can be derived (Bojanc & Jerman-Blažič 2008b). This improves the quality of data, including costs, benefits, risks, and non-monetary criteria, as well as the reliability of the assessment result (Schilling & Werners 2015). Hence, I propose **DR 2: "Data integrity":** *A multiple-criteria assessment tool for information security investments should use valid sources to provide reliable assessment results.*

As multiple-criteria assessment tools are intended to offer solutions tailored to individual companies and use cases, they must be well-applicable in different contexts and for different users (Bodin et al. 2005). For this, such tools need to be able to assess and compare several InfoSec investments as well as individual ones (Kühnel et al. 2021). Therefore, a comprehensible, transparent, and systematic assessment process should build a cornerstone of the model (Smith & Kruger 2010). Thereby, the users conduct the assessments correctly, collaboration within a company becomes possible, and the results can be communicated to and understood by co-workers and superiors (Weishäupl et al. 2015b). Yet, the assessments need to remain time-efficient so that they can be well-integrated into a company's business (Bojanc et al. 2012). To address this, I infer **DR 3: "Usability":** *A multiple-criteria assessment tool for information security investments should be well-applicable in a company's context.*

Multiple-criteria assessment tools should be feasible to gather information from both individual experts as well as co-workers from other departments in a company (Lee et al. 2011). Thereby, on the one hand, a user is offered to contribute their own professional experience (Sheen 2010), as his InfoSec knowledge regarding an investment option. On the other hand, co-workers from a different department, in which the security measure might, for example, impact their business, can contribute the necessary multiple criteria to assess the investments more precisely than an InfoSec expert could (Dor & Elovici 2016, Weishäupl et al. 2018). Accordingly, I propose **DR 4: "Accessibility":** *A multiple-criteria assessment tool for information security investments should promote the assessment and collaboration in a company.*

In the following, the DPs are described with again referencing to the literature of the SLR. In addition, further implications arising from the expertise I have gained from researching the theoretical background are discussed. In doing so, possible addressees, areas of application, and connections between the DPs and DRs are discussed.

DP 1: "Cost integration": *A multiple-criteria assessment tool for information security investments should enable the definition of the scope of relevant costs in order to quantify and assess the implementation costs for information security measures.* For the assessment and quantification of implementation costs, it is first necessary to clearly define them within the multiple-criteria assessment tool (Huang et al. 2008, Wang et al. 2012). One should consider whether, for example, only the purchase costs or also

the costs resulting from the maintenance of the InfoSec measure should be examined (Kuehnel et al. 2022). When quantifying only the purchase costs, it is probably easier to consider their monetary value than the costs arising from the maintenance of a security measure. Data for the cost assessment could be supplied by the purchasing department of a company as well as the departments affected by the security measure.

DP 2: "Benefit integration": *A multiple-criteria assessment tool for information security investments should enable the definition of the scope of relevant benefits in order to quantify and assess the benefits resulting from the implementation of information security measures.* As with the implementation costs, it is important to define what includes the benefits of an InfoSec investment and how those can be derived and monetized to accurately determine them (Huang & Behara 2013). Here, monetization poses a greater challenge than monetizing the implementation costs (Gordon & Loeb 2006). The benefits of an InfoSec investment mainly result from the prevented costs of an InfoSec breach (Kuehnel et al. 2022). A forecast of potential incident costs could therefore be helpful (Huang et al. 2008). In addition, the benefit can also be considered in comparison to the available budget of an IT department (Gordon & Loeb 2006). The simultaneous visualization of the prevented costs, implementation costs, and the budget available to the IT department within a multiple-criteria assessment tool could thereby help to conduct a trade-off for an InfoSec investment.

DP 3: "Risk integration": *A multiple-criteria assessment tool for information security investments should enable the definition of the scope of relevant risks in order to quantify and assess the risks mitigated by an information security measure.* For InfoSec risks to be assessed, the potentially affected information themselves should first be defined, assessed, and quantified (Huang et al. 2008, Sonnenreich et al. 2006). Based on this, the risks can be quantified or monetized (Gordon & Loeb 2006). The necessary details for the assessment of information and InfoSec risks should ideally originate from the department affected by the InfoSec investment as well as the IT or InfoSec department in particular. This allows both functional and InfoSec expertise to be drawn on.

DP 4: "Integration of non-monetary criteria": *A multiple-criteria assessment tool for information security investments should enable the definition, quantification, and assessment of non-monetary criteria in order to make the assessment of information security investments become more comprehensive.* InfoSec breaches entail a strong intangible impact on a company's business (Statista 2024). This impact should also be included in the assessment of an InfoSec investment. In addition, the multiple-criteria assessment tool should also enable the integration and assessment of non-monetary criteria that reveal the impact of a security measure in a business or business processes of the affected departments (Matschak et al. 2023). Exemplary non-monetary criteria could be 'process complexity' or 'employee satisfaction'. Those could also influence the performance and profitability of a company (Kühnel et al. 2021). For the definition and assessment of such non-monetary criteria, the expertise of the employees of the affected departments of a company is required (Matschak et al. 2023).

DP 5: "Data sources": *A multiple-criteria assessment tool for information security investments should consider various types of data sources as assessment foundations in order to provide the necessary data for a multiple-criteria assessment.* The use of recorded historical data for the assessment of InfoSec investments offers a

high level of reliability (Bojanc & Jerman-Blažič 2008a). However, such data may be lacking or incomplete in many companies, especially concerning non-monetary criteria (Franqueira et al. 2010). Subjective data must therefore be used to ensure a complete assessment (Beresnevichiene et al. 2010). For this purpose, employees of an affected department could, due to their experience, provide data regarding the assessment criteria. In addition, InfoSec experts could provide data for the assessment of the InfoSec investment, also relying on their personal experience with the topic of InfoSec.

DP 6: "Data quality": *A multiple-criteria assessment tool for information security investments should ensure that the data and assessment foundation is valid and accurate in order to be able to use the assessment result as foundation for investment decisions.* The validity of recorded historical data as well as the validity of the assessment result derived from such data poses less of a challenge in comparison with subjective data, based on one's personal experience (Bojanc & Jerman-Blažič 2008a). With the latter, attention must be paid to the consistency of the data to achieve reliable results (Franqueira et al. 2010). This is especially important regarding the communication of the assessment results to superiors (Beresnevichiene et al. 2010). Managers need to be able to rely on the results of the assessment when making investment decisions.

DP 7 "Scope of security measures": *A multiple-criteria assessment tool for information security investments should enable the assessment of bundles of information security measures as well as information security measures in comparison to each other in order to identify the security solution that applies best to a company's use case.* In practice, assessments and decisions on InfoSec investments are often not made in isolation (Čapko et al. 2014, Kühnel et al. 2021). Either there are several providers of security measures, various and different kind of security measures, or a bundle of security measures that needs to be assessed (Kühnel et al. 2021, Matschak et al. 2023). The assessment tool should therefore consider the complexity of realistic assessment situations and allow the users to keep an overview of the assessment scope.

DP 8: "Feasible assessment": *A multiple-criteria assessment tool for information security investments should be comprehensible and user-friendly in order to promote the implementation of an assessment tool in a company and to make the decision process traceable.* Reduced complexity when using the assessment tool, for example through minimal calculation effort for the user, increases its user-friendliness and acceptance (Khansa & Liginlal 2009). This is particularly important for those employees who engage with the assessment tool only occasionally and do not have much experience with the assessment of InfoSec investments (Schatz & Bashroush 2017). Implementing this principle can therefore increase the application and establishment of the multiple-criteria assessment tool in a company.

DP 9: "Structured assessment": *A multiple-criteria assessment tool for information security investments should be systematic, structured, and transparent in order to ensure a consistent assessment process.* A systematic and transparent assessment tool increases its comprehensibility and could thus ensure that the assessment is carried out correctly by the respective user (Herath & Herath 2008). This increases the chances of receiving a high-quality and valid assessment result (Huang & Huang 2014). In addition, the transparency of the multiple-criteria assessment tool helps to communicate

the tool itself as well as its results within a company, as it makes them easier to understand (Herath & Herath 2008). This enables employees to better justify investment decisions for or against an InfoSec investment towards their superiors.

DP 10: "Application effort": *A multiple-criteria assessment tool for information security investments should minimize the timely effort required for the application of assessments in order to promote its application.* The assessment of InfoSec investments does not only concern the InfoSec department of a company (Matschak et al. 2023). It affects all employees and departments working in businesses or with processes that are affected by the investment in and implementation of InfoSec measures (Bojanc et al. 2012). Therefore, these employees should also participate in the assessment. The effort this assessment requires, however, is added to their daily workload. Hence, to prevent the assessment tool from being ignored or incorrectly applied, it needs to take up as little time as possible (Schatz & Bashroush 2017). For example, it would be helpful if the assessment process could be paused in between to spread the effort over time. This principle applies to both data procurement and the assessment itself.

DP 11: "Cooperation in a company": *A multiple-criteria assessment tool for information security investments should enable the cooperation and communication within an assessment process in a company by the possible integration of multiple co-workers and departments in order to use the entire organization's expertise.* By the integration of co-workers within the assessment tool, the assessment can benefit from their professional or InfoSec expertise (Bojanc et al. 2012). The multiple-criteria assessment tool should enable this level of cooperation. In this context, it could be useful for a successful assessment to define a specific project manager or admin to individual assessment projects within the assessment tool. This person should have a particularly high level of functional expertise or experience with investment assessments (Bojanc et al. 2012). Additionally, it may also be beneficial for both the project manager and other users of the multiple-criteria assessment tool to be able to provide information on their degree of confidence in their assessment (Huang et al. 2014). This would allow the assessments of certain people to be prioritized higher than those of others and could therefore offer a more reliable assessment result. Following the assessment, its results should be prepared in such a way that they can be easily and transparently communicated to both colleagues and superiors (Franqueira et al. 2010).

5 Evaluation

For the evaluation of the DT and the DPs in particular, an MFG following the approach of Morgan (1997) was conducted. The MFG consisted of eight IS and InfoSec experts from academia. For the determination of the sample size of the focus group, the "10±2 rule" by Hwang and Salvendy (2010) was applied. The focus group discussed the evaluation criteria proposed by Möller et al. (2020). For one, these consist of the criteria of 'prescriptiveness' and 'abstractedness' (Gregor & Hevner 2013), which were positively highlighted in the discussion. One expert gave additional advice to supplement the DT with specific design features (DFs), which could provide additional functional instructions for the design of multiple-criteria assessment tools. Thereby, "[…] the experience

and expertise of all company employees who work with such a tool, e.g. as part of an IT tool, must be considered," stated one MFG participant.

In addition, Möller et al. (2020) propose to evaluate the reusability of the DPs by applying the evaluation criteria of 'accessibility', 'importance', 'novelty and insightfulness', 'actability and guidance', and 'effectiveness' following Iivari et al. (2021). The 'accessibility' was positively evaluated, with a few qualitative remarks on the wording of the DPs, especially DP 1, 5, and 10. The remarks were implemented after the evaluation. The 'importance' was considered particularly high during the discussion and the need of a comprehensive assessment tool was highlighted. The 'novelty and insightfulness' was seen as good, especially in the case of DP 4, 7, and 11. Concerning 'actability and guidance', there were a few comments on the conceptual clarity of DP 2 and 5, which were also implemented after the evaluation. The 'effectiveness' was positively emphasized. One participant mentioned that the DT "[…] allows to make well informed and more robust decisions for InfoSec investments.". The aspect of being able to use the DT to develop assessment tools that make comprehensive investment decisions while keeping the entire company in mind was emphasized. After making the small adjustments according to the evaluation, I am now convinced that the DT fully complies with the evaluation criteria proposed by Möller et al. (2020).

6 Discussion

Only a few design theories in the field of InfoSec discussed aspects of economic efficiency. Among these, to the best of my knowledge, none of them address the task of multiple-criteria assessment of InfoSec investments. This study takes up on this task, presents such a DT, and therefore answers the research question: *What are design requirements and design principles for the development of a multiple-criteria assessment tool for information security investments?* I presented the results in the context of a DSR approach and conducted a complete iteration of a literature-driven design cycle. To ensure scientific rigor, the method of DP development of Möller et al. (2020) was applied, based on an SLR following vom Brocke et al. (2009). This procedure was presented comprehensively and transparently. Hereby, the DT for multiple-criteria assessment tools for InfoSec investments, consisting of DRs and DPs, is the result of a complete iteration.

The broad perspective of the DT could be of high interest to both scientists and practitioners. For the IS community, a new theoretical foundation based on a DT is systematically developed that can be successfully built upon in further research. For both scientists and practitioners, the DT contributes to the prescriptive knowledge base (Gregor & Hevner 2013). At the same time, it retains an appropriate degree of abstraction and that would allow the DT to be transferred to various software artifacts in practice without committing to a specific instantiation (Gregor & Hevner 2013).

The DT is particularly distinctive, as it draws on both monetary and non-monetary criteria. In the past, the economic assessment of InfoSec investments has focused on traditional financial criteria such as costs and benefits (Schatz & Bashroush 2017). However, the fact that non-monetary criteria also affect a company's performance and

therefore its profitability has largely been ignored (Heidt et al. 2019). In addition, the DT focuses on factors relating to acceptance and usability. This is of particular interest to practitioners, as software artifacts derived from the DT should therefore be easy to integrate and establish in a company. The success of the DT presented in this paper is also reflected in the positive results of the evaluation, especially regarding the criteria of 'importance', 'novelty and insightfulness', and 'effectiveness.

However, the study also contains a few limitations. As already described, the knowledge base of the DT consists mostly of literature. Although this procedure complies with Möller et al.'s (2020) method and additional expert feedback was gathered through the evaluation of the DT within a moderated focus group, the DT is based on a theoretical foundation. To strengthen the empirical foundation, future research should therefore have a look at practice and include the personal expertise and knowledge of potential users. Qualitative methods, such as of semi-structured interviews or case study research, would be ideal for this (Möller et al. 2020). Furthermore, although this iteration and DT are now complete (Möller et al. 2020), some improvements could still be made in further research. This has already been indicated by a few comments made during the evaluation. The deployment of qualitative methods could also be used to specifically determine which non-monetary criteria should be considered, particularly in DR 1: "Efficiency".

To illustrate the usefulness of the multiple-criteria DT in practice, it could also be instantiated as part of a software artifact. So far and to the best of my knowledge, there is no functional design foundation for this. Therefore, researchers could extend the DT by identifying and presenting specific DFs. Based on these, a software artifact could be built. A quantitative evaluation of the resulting DT could then be paired with a case study to test and evaluate the software artifact.

7 Conclusion

In this paper, the results of a complete DSR project to develop a DT consisting of 4 requirements and 11 principles were presented. The research is based on an SLR and the results were evaluated within an MFG of IS and InfoSec experts from academia. The evaluation focused on the evaluation criteria of Iivari et al. (2021) and concluded with positive feedback from the academic experts. This study, therefore, offers a valid foundation of design knowledge for research and practice. The DT can be adapted to develop newly emerging multiple-criteria assessment tools for InfoSec investments in the scientific field and offers a basis for future instantiations of software artifacts.

Acknowledgments

The project on which this study is based was funded by the German Federal Ministry of Education and Research under grant number 16KIS1331. The responsibility for the content of this publication lies with the authors.

Appendix

Table 2. Concept Matrix

Publication	DP 1	DP 2	DP 3	DP 4	DP 5	DP 6	DP 7	DP 8	DP 9	DP 10	DP 11
Neubauer & Hartl 2009	x	x		x	x	x	x	x		x	
Sheen 2010		x	x		x	x	x	x			
Smith & Kruger 2010	x	x	x	x				x			x
Capko et al. 2014			x				x				
Buck & Hanf 2008	x	x	x	x		x	x		x		x
Wang et al. 2012		x									
Huang et al. 2014		x	x				x		x		x
Huang et al. 2008	x	x	x		x						
Weishäupl et al. 2018					x			x			x
Bojanc & Jerman-Blazic 2008a	x	x			x	x	x				
Lee et al. 2011	x	x	x		x				x		x
Huang & Behara 2013	x	x					x	x			
Bojanc et al. 2012	x	x					x			x	
Herath & Herath 2008	x	x			x				x		x
Schilling & Werners 2015		x	x		x	x	x	x		x	
Matschak et al. 2023				x	x	x	x	x	x	x	
Weishäupl et al. 2015b	x	x									x
Beresnevichiene et al. 2010	x	x	x		x	x	x	x	x		
Bodin et al. 2005	x	x		x	x		x	x			
Bojanc & Jerman-Blazic 2008b	x	x	x		x	x				x	
Dor & Elovici 2016	x				x	x					x
Fielder et al. 2016	x	x						x			
Gordon & Loeb 2006	x	x	x		x						
Khansa & Liginlal 2009			x			x		x			
Kühnel et al. 2021		x		x	x	x	x				
Schatz & Bashroush 2017	x	x	x	x	x		x	x	x	x	
Sonnenreich et al. 2006	x	x	x		x	x			x		
Franqueira & Houmb 2010	x	x			x						

References

Balozian, P., Burns, A. J. & Leidner, D. E. (2023), 'An Adversarial Dance, Toward an Understanding of Insiders' Responses to Organizational Information Security Measures', *Journal of the Association for Information Systems* **24**(1), 161–221.

Bandyopadhyay, T. & Zafar, H. (2017), Influence of Information Overload on IT Security Behavior, A Theoretical Framework, *in* 'Proceedings of the Americas Conference on Information Systems.

Baskerville, R. & Pries-Heje, J. (2010), 'Explanatory Design Theory', *Business Information Systems Engineering* **2**(5), 271–282.

Beresnevichiene, Y., Pym, D. & Shiu, S. (2010), Decision Support for Systems Security Investment, *in* 'IEEE/IFIP Network Operations and Management Symposium Workshops', IEEE.

Bodin, L. D., Gordon, L. A. & Loeb, M. P. (2005), 'Evaluating information security investments using the analytic hierarchy process', *Communications of the ACM* **48**(2), 78–83.

Bojanc, R. & Jerman-Blažič, B. (2008a), 'An economic modelling approach to information security risk management', *International Journal of Information Management* **28**(5), 413–422.

Bojanc, R. & Jerman-Blažič, B. (2008b), 'Towards a standard approach for quantifying an ICT security investment', *Computer Standards & Interfaces* **30**(4), 216–222.

Bojanc, R., Jerman-Blažič, B. & Tekavčič, M. (2012), 'Managing the investment in information security technology by use of a quantitative modeling', *Information Processing & Management* **48**(6), 1031–1052.

Buck, K. & Hanf, D. (2008), Applying ROI Analysis to Support SOA Information Security Investment Decisions, *in* 'Proceedings of the IEEE Conference on Technologies for Homeland Security', IEEE.

Čapko, Z., Aksentijević, S. & Tijan, E. (2014), Economic and financial analysis of investments in information security, *in* '37th International Convention on Information and Communication Technology, Electronics and Microelectronics', MIPRO.

Chen, P., Chern, C., Chen, C. & Tzeng, G. (2013), IT Portfolio Investment Evaluation on ECommerce Solution Alternatives, *in* 'Proceedings of the Pacific Asia Conference on Information Systems', PACIS.

Cooper, H. M. (1988), 'Organizing knowledge syntheses, A taxonomy of literature reviews', *Knowledge in Society* **1**(1), 104–126.

Dhillon, G., Talib, Y. Y. A. & Picoto, W. N. (2020), 'The Mediating Role of Psychological Empowerment in Information Security Compliance Intentions', *Journal of the Association for Information Systems* **21**(1), 152–174.

Dor, D. & Elovici, Y. (2016), 'A model of the information security investment decision-making process', *Computers & Security* **63**, 1–13.

Ebbers, F., Hacks, S. & Thakurta, R. (2021), The Business Impact of IIoT Vulnerabilities, in 'Proceedings of the Pacific Asia Conference on Information Systems', PACIS.

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C. & Smeraldi, F. (2016), 'Decision support approaches for cyber security investment', *Decision Support Systems* **86**, 13–23.

Franqueira, V. N. L., Houmb, S. H. & Daneva, M. (2010), Using Real Option Thinking to Improve Decision Making in Security Investment, *in* 'Proceedings of the Conference on the Move to Meaningful Internet Systems, OTM.

Fu, K. K., Yang, M. C. & Wood, K. L. (2016), 'Design Principles, Literature Review, Analysis, and Future Directions', *J. Mech. Des* **138**(10).

Gordon, L. A. & Loeb, M. P. (2006), 'Budgeting process for information security expenditures', *Commun. ACM* **49**(1), 121–125.

Gregor, S. & Hevner, A. R. (2013), 'Positioning and Presenting Design Science Research for Maximum Impact', *MIS Quarterly* **37**(2), 337–355.

Guggenmos, F., Häckel, B., Ollig, P. & Stahl, B. (2022), 'Security First, Security by Design, or Security Pragmatism – Strategic Roles of IT Security in Digitalization Projects', *Computers & Security* **118**.

Heidt, M., Gerlach, J. P. & Buxmann, P. (2019), A Holistic View on Organizational IT Security, The Influence of Contextual Aspects during IT Security Decisions, *in* 'Proceedings of the Hawaii International Conference on System Sciences', PACIS.

Herath, H. S. B. & Herath, T. C. (2008), 'Investments in Information Security, A Real Options Perspective with Bayesian Postaudit', *Journal of Management Information Systems* **25**(3), 337–375.

Huang, D. C. & Behara, Ravi S. (2013), 'Economics of information security investment in the case of concurrent heterogeneous attacks with budget constraints', *International Journal of Production Economics* **141**(1), 255–268.

Huang, D. C., Behara, R. S. & Goo, J. (2014), 'Optimal information security investment in a Healthcare Information Exchange, An economic analysis', *Decision Support Systems* **61**, 1–11.

Huang, D. C., Hu, Q. & Behara, R. S. (2008), 'An economic analysis of the optimal information security investment in the case of a risk-averse firm', *International Journal of Production Economics* **114**(2), 793–804.

Huang, K. Y. & Huang, Y. C. (2014), An efficient multi-criteria decision-making approach based on hybridizing data mining techniques, *in* 'Proceedings of the Pacific Asia Conference on Information Systems', PACIS.

Hwang, W. & Salvendy, G. (2010), 'Number of people required for usability evaluation', *Communications of the ACM* **53**(5), 130–133.

Iivari, J., Rotvit Perlt Hansen, M. & Haj-Bolouri, A. (2021), 'A proposal for minimum reusability evaluation of design principles', *European Journal of Information Systems* **30**(3), 286–303.

Jiang, Y., Jeusfeld, M. A., Ding, J. & Sandahl, E. (2023), 'Model-Based Cybersecurity Analysis', *Bus Inf Syst Eng* **65**(6), 643–676.

Khansa, L. & Liginlal, D. (2009), 'Valuing the flexibility of investing in security process innovations', *European Journal of Operational Research* **192**(1), 216–235.

Kitchenham, B., Pearl Brereton, O., Budgen, D., Turner, M., Bailey, J. & Linkman, S. (2009), 'Systematic literature reviews in software engineering – A systematic literature review', *Information and Software Technology* **51**(1), 7–15.

Kuehnel, S., Sackmann, S., Damarowsky, J. & Boehmer, M. (2022), EconBPC, A Tool for Activity-based Monetary Assessment and Visualization of Security and Compliance Measures in Business Processes, *in* 'Proceedings of the Best Dissertation Award, Doctoral Consortium, and Demonstration & Resources Track at BPM 2022,

Co-located with 20th International Conference on Business Process Management (BPM 2022)', Münster, Germany, CEUR-WS Vol-3216, pp. 127-131.
Kuehnel, S., Trang, S. T.-N. & Lindner, S. (2019), 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) 'Proceedings of the International Conference on Conceptual Modeling (ER 2019)', Salvador, Brazil, Lecture Notes in Computer Science (11788), vol 11788. Springer, Cham, pp. 378-386. https://doi.org/10.1007/978-3-030-33223-5_31.
Kühnel, S., Sackmann, S., Trang, S., Nastjuk, I., Matschak, T., Niedzela, L. & Nake, L. (2021), Towards a business process-based economic evaluation and selection of IT security measures, *in* 'Proceedings of the First International Workshop on Current Compliance Issues in Information Systems Research (CIISR'21), Co-located with the 16th International Conference on Wirtschaftsinformatik (WI'21)', Essen, Germany (online), CEUR-WS Vol-2966, pp. 7–21.
Lee, Y. J., Kauffman, R. J. & Sougstad, R. (2011), 'Profit-maximizing firm investments in customer information security', *Decision Support Systems* **51**(4), 904–920.
Li, H., Yoo, S. & Kettinger, W. (2019), The Changing Tides of Investments and Strategies and Their Impacts on Security Breaches, *in* 'Proceedings of the International Conference on Information Systems', ICIS, pp. 1–16.
Llansó, T., McNeil, M. & Noteboom, C. (2019), Multi-Criteria Selection of Capability-Based Cybersecurity Solutions, *in* 'Proceedings of the Hawaii International Conference on System Sciences', HICSS.
Matschak, T., Nastjuk, I., Niedzela, L., Kuehnel, S. & Trang, S. (2023), A Process-Based Approach to Information Security Investment Evaluation, Design, Implementation, and Evaluation, *in* 'Proceedings of the Americas Conference on Information Systems', AMCIS 2023 Proceedings 30.
Mithas, S., Tafti, A. & Mitchell, W. (2013), 'How a firm's competitive environment and digital strategic posture influence digital business strategy', *MIS Quarterly* **37**(2), 511–536.
Möller, F., Guggenberger, T. & Otto, B. (2020), Towards a Method for Design Principle Development in Information Systems, *in* 'Lecture Notes in Computer Science', Springer, pp. 208–220.
Morgan, D. L. (1997), *Focus Groups as Qualitative Research*, SAGE Publications.
Mujinga, M., Eloff, M. M. & Kroeze, J. H. (2017), A Socio-Technical Approach to Information Security, *in* 'Proceedings of the Americas Conference on Information Systems', PACIS.
Neubauer, T. & Hartl, C. (2009), On the Singularity of Valuating IT Security Investments, *in* 'Eighth IEEE/ACIS International Conference on Computer and Information Science', IEEE, pp. 549–556.
Niedzela, L., Kuehnel, S., Nastjuk, I., Matschak, T., Sackmann, S. & Trang, S. (2023), A Qualitative Study on Acceptance Factors of Economic Approaches on IT Security Investment Decisions, *in* 'Proceedings of the Americas Conference on Information Systems, AMCIS 2023, Proceedings 16.
Niedzela, L., Nake, L. & Matschak, T. (2022), Categories of Approaches for IT Security Investment Decisions, A systematic literature review, *in* 'Proceedings of the In-

ternational Workshop on Current Compliance Issues in Information Systems Research (CIISR), International Conference on Wirtschaftsinformatik', WI 2022, Proceedings 4.
Schatz, D. & Bashroush, R. (2017), 'Economic valuation for information security investment, a systematic literature review', *Information Systems Frontiers* **19**(5), 1205–1228.
Schilling, A. & Werners, B. (2015), Optimal Information Security Expenditures Considering Budget Constraints, *in* 'Proceedings of the Pacific Asia Conference on Information Systems', PACIS.
Shao, X., Siponen, M. & Liu, F. (2020), 'Shall we follow? Impact of reputation concern on information security managers' investment decisions', *Computers & Security* **97**, 1–10.
Shao, X., Siponen, M. & Pahnila, S. (2019), To Calculate or To Follow Others, How Do Information Security Managers Make Investment Decisions?, *in* 'Proceedings of the Hawaii International Conference on System Sciences', HICSS.
Sheen, J. N. (2010), Information security investment decision by fuzzy economics, *in* 'Proceedings of the International Conference on Information Sciences and Interaction Sciences', ICIS.
Smith, E.H. & Kruger, H.A. (2010), A framework for evaluating IT security investments in a banking environment, *in* 'Information Security for South Africa', ISSA, IEEE.
Sonnenreich, W., Albanese, J. & Stout, B. (2006), 'Return On Security Investment (ROSI). A Practical Quantitative Model', *Journal of Research and Practice in Information Technology* **38**(1), 45–56.
Srinidhi, B., Yan, J. & Tayi, G. K. (2015), 'Allocation of resources to cyber-security, The effect of misalignment of interest between managers and investors', *Decision Support Systems* **75**, 49–62.
Statista (2024), https,//de.statista.com/statistik/daten/studie/444719/umfrage/schaeden-durch-computerkriminalitaet-in-deutschen-unternehmen/. Accessed: 13.05.2024.
Van Looy, A. & Shafagatova, A. (2016), 'Business process performance measurement, a structured literature review of indicators, measures and metrics', *SpringerPlus* **5**(1), 2–24.
Vedadi, A., Warkentin, M. & Dennis, A. (2021), 'Herd behavior in information security decision-making', *Information & Management* **58**(8), p. 103526.
Vom Brocke, J., Simons, A., Niehaves, B., Riemer, K., Plattfaut, R. & Cleven, A. (2009), Reconstructing the Giant. On the Importance of Rigour in Documenting the Literature Search Process, *in* 'European Conference on Information Systems', ECIS.
Walls, J. G., Widmeyer, G. R. & El Sawy, O. A. (1992), 'Building an Information System Design Theory for Vigilant EIS', *Information Systems Research* **3**(1), 36–59.
Wang, J., Ding, B., Ren, Y. F., Zheng, J. X. & Guo, H. Y. (2012), Valuing Information Security Investment, A Real Options Approach, *in* 'Fifth International Conference on Business Intelligence and Financial Engineering', pp. 279–284.
Wanner, J., Heinrich, K., Janiesch, C. & Zschech, P. (2020), How Much AI Do You Require? Decision Factors for Adopting AI Technology, *in* 'Proceedings of the International Conference on Information Systems', ICIS.

Weishäupl, E., Yasasin, E. & Schryen, G. (2015a), A Multi-Theoretical Literature Review on Information Security Investments using the Resource-Based View and the Organizational Learning Theory, *in* 'Proceedings of the International Conference on Information Systems', ICIS.

Weishäupl, E., Yasasin, E. & Schryen, G. (2015b), IT Security Investments Through the Lens of the Resource-based view, A new theoretical model and literature review, *in* 'Proceedings of European Conference on Information Systems', ECIS.

Weishäupl, E., Yasasin, E. & Schryen, G. (2018), 'Information security investments, An exploratory multiple case study on decision-making, evaluation and learning', *Computers & Security* **77**, 807–823.

Zafar, H. & Clark, J. G. (2009), 'Current State of Information Security Research In IS', *Communications of the Association for Information Systems* **24**(1), 571–596.