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

Keynote

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

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

1 Introduction

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

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

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

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

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

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

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

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

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

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

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

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

2.1 The Annual Loss Exposure

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

2.2 Return on Security Investment

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

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

2.3 Return on Information Security Investment

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

2.4 Adapted Loss Database

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

2.5 Cyber Investment Analysis Methodology

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

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

2.6 Security Attribute Evaluation Method

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

3 Limitations of Existing Evaluation Methods for IT Security Measures

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5 Conclusion

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

References

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

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

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

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

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