

Integration of Data Envelopment Analysis in Business Process Models: A Novel Approach to Measure Information Security

Agnes Åkerlund and Christine Große^a

Department of Information Systems and Technology, Mid Sweden University, Holmgatan 10, Sundsvall, Sweden

Keywords: Data Envelopment Analysis, Information Security, Business Process, BPMN, Human Factor.

Abstract: This article explores the question of how to measure information security. Organisational information security is difficult to evaluate in this complex area because it includes numerous factors. The human factor has been acknowledged as one of the most challenging factors to consider in the field of information security. This study models the application of data envelopment analysis to business processes in order to facilitate the evaluation of information security that includes human factors. In addition to the model, this study demonstrates that data envelopment analysis provides an efficiency measure to assess the information security level of a business process. The novel approach that is proposed in this paper is exemplified with the aid of three fictive processes. The Business Process Model and Notation has been used to map the processes because it facilitates the visualisation of human interactions in processes and the form of the processed information. The combination of data envelopment analysis with process modelling and analyses of process deficiencies and threats to information security enables the evaluation of information security to include human factors in the analyses. Moreover, it provides a measure to benchmark information security in organisational processes.


1 INTRODUCTION

The inclusion of human factors in organisational efforts to ensure information security (InfoSec) is both necessary and challenging. One obstacle to such integration is that the standard definition of InfoSec does not explicitly include human factors in evaluations of information processing (Lundgren and Möller, 2019). In addition, the human factor can exert two opposite effects on organisational InfoSec. First, employees can reduce risks to InfoSec in an organisation when complying with policies (Bulgurcu, Cavusoglu and Benbasat, 2010; Lundgren and Möller, 2019). Second, the human interaction with information poses a major threat to its security (Gonzalez and Sawicka, 2002; Vroom and von Solms, 2004). Therefore, in addition to external threats to InfoSec, organisations must contend with internal threats that emerge from human interaction with information during business processes. This paper aims to address the need to enlarge the perspective of InfoSec. It focuses on human factors in business processes and proposes a novel approach to evaluate and benchmark InfoSec in organisations.

The new approach applies data envelopment analysis (DEA) to business processes. Since the Business Process Model and Notation (BPMN) facilitates both the identification of human interaction with information in processes and the form of the processed information, it offers valuable input for the following DEA.

The DEA is a popular tool of management analysis to evaluate the efficiency and performance of businesses or operations, such as mass productions or logistics (Arunyanart, Ohmori and Yoshimoto, 2015; da Silva, Marins, Tamura and Dias, 2017; Zheng and Park, 2016). To date, DEA has not been studied as tool for examining InfoSec among processes. The present study addresses this gap in InfoSec research.

Subsequent to the background and method sections, Section 4 describes the proposed model in more detail. An example implementation evaluates the model and demonstrates the benchmarking of business processes. Then, Section 5 discusses the suggested approach and its practical applicability. A brief conclusion completes the study.

^a  <https://orcid.org/0000-0003-4869-5094>

2 BACKGROUND

2.1 Human Factors in InfoSec

The cornerstones of InfoSec are the triad of confidentiality, integrity and availability. The ISO/IEC 27000:2018 standard defines confidentiality as the principle that information is available for the right persons and protected from disclosure to unauthorized individuals, processes or entities. Integrity indicates that information is correct and complete, and availability is achieved when information is accessible and useable by certified users (ISO 27000:2018; Laybats and Tredinnick, 2016; Lundgren and Möller, 2019; Paliszkievicz, 2019).

To ensure proper levels of InfoSec, organisational efforts need to consider internal and external threats. Apart from external threats to InfoSec, human aspects warrant particular attention in order to reduce InfoSec risks (e.g. Pereira and Santos, 2015). Since information systems are socio-technical systems that involve both technical and human components in interaction, such systems rely on not only appropriate technical measurements for ensuring InfoSec but also the awareness of human operators. Thus, human behaviour is crucial for maintaining adequate InfoSec (Gonzalez and Sawicka, 2002; Nyman and Große, 2019; Vroom and von Solms, 2004). Metalidou et al. (2014) have emphasised that '[i]nformation security has not been given enough attention in the literature in terms of the human factor effect' and encouraged further investigation in this field.

From the perspective of human factors as internal threats, one risk emerges from people who access programs and information systems at an organisation.

One measure to prevent unauthorised access to information flows is to assign permission to certain employees by an administration department (Mitrovic, 2005). Every human interaction with information in a system poses a certain risk to InfoSec, and this risk increases with each person who has access to the information. Hence, in business processes, the number of people who edit information should be reduced if possible (Hwang and Cha, 2018; Laybats and Tredinnick, 2016).

Other mitigation strategies consider eliminating the manual control of information and its varying formats. First, manual control, which depends on people, carries a risk of violating InfoSec (Venegas, 2007). Second, the change of the information format can incorporate a threat to InfoSec if the data is not properly converted. The risk of losing or improperly changing data or information in a transformation can

be reduced by decreasing human interaction with processed information during business processes (Lawrence et al., 2000; Venegas, 2007)

Moreover, passwords have proven to be an effective way to enhance InfoSec (Wood, 1983). Although text-based passwords are the most common type, organisational password policies can require special characters or numbers. The advantage derives from the effect of more characters reducing the success of guessing the password (Komanduri et al., 2011). However, passwords that are more complicated to comply with such policies accordingly have lower usability (AlFayyadh, Thorsheim, Jøsang, and Klevjer, 2012). Such decrease in usability implies that employees struggle to remember passwords and therefore tend to write them down, which in turn poses a threat to InfoSec.

However, measuring InfoSec including the selection of metrics is perceived as challenging and far from obvious (Houngbo and Hounsou, 2015). Research has acknowledged a need for measurable InfoSec by design (e.g. Cohen, 2011; Stolfo et al., 2011) and argued that proper measurements, for example regarding human factors, are necessary to improve decision making (Zalewski et al., 2014).

2.2 Information in Business Processes

Several key organisational indicators depend on information that is generated alongside business processes, such as supply chains. Examples of such key indicators are the productivity of industrial manufacturing or the innovation of new services. In such contexts, people depend on proper information to proceed, which also affects the efficiency of an organisation (Badenhorst, Maurer, and Brevis-Landsberg, 2013). To achieve an appropriate information flow, several tools have been developed to visualise the flows of information and material within and between organisations. A simple tool for mapping value streams can help to identify waste within processes, which can facilitate mitigation and heightened efficiency (Garza-Reyes, Torres Romero, Govindan, Cherrafi, and Ramanathan, 2018).

The BPMN, which is an ISO standard, is another tool for modelling a business process and its activities (ISO 19510:2013; Geiger, Harrer, Lenhard, and Wirtz, 2018). Previous research has demonstrated the usefulness of BPMN to include considerations regarding InfoSec in business process models. Such studies have, for example, addressed the integration of the General Data Protection Regulation (Bartolini, Calabro and Marchetti, 2019) or the integrated quality and InfoSec management in small and medium-sized

enterprises (Große, 2016). The BPMN not only assists in the identification of human interaction with processed information but also indicates the form of the processed information. The interaction with information during a business process can occur manually by a human operator or automatically through a technical information system. The BPMN provides several categories of elements that yield a detailed representation of the information processing alongside an organisational process.

2.3 Data Envelopment Analysis

Data envelopment analysis was first developed by Charnes, Cooper and Rhodes (CCR) (1978). This analysis enables analysts to calculate the efficiency of an output from non-parametric inputs, such as resources. Figure 1 illustrates such analysis, which supports organisations to evaluate their process efficiency in order to find weaknesses and strengths in processes, which can indicate potential for further development in a competitive environment (Zhu, 2014).

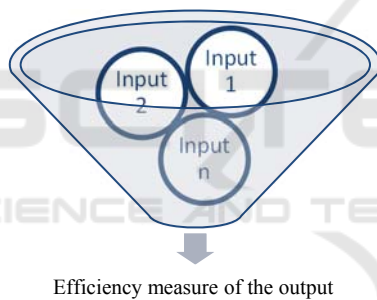


Figure 1: Data envelopment analysis.

In DEA, a business process is called a decision-making unit (DMU), each of which has inputs and outputs (Zhu, 2014). An ideal DMU (IDMU) constitutes the perfect DMU that uses the lowest input to provide the maximum output. Such IDMU is the most efficient option compared to other DMUs but often exists solely as a virtual representation (Wang and Luo, 2006).

The efficiency measure is calculated from the weighted sum of inputs and outputs. The weights are assigned to maximise the efficiency score. There are different models within DEA, such as the classic CCR model or the Assurance Region I (ARI) model. The CCR model assumes that inputs and outputs are based on a constant return to scale. The efficiency measure emerges from the relationship between inputs and outputs. One problem with the CCR model is that it allows weights equal to zero; consequently, important

inputs or outputs can be neglected (Mecit and Alp, 2013). In contrast, the ARI model can use weight restrictions to mitigate this problem. The ARI model maximises efficiency scores through the sum for the output weights multiplied by the output values. Whereas the former model views inputs as resources that are required to perform a process and outputs as the result, the latter DEA model is used to evaluate the relative efficiency between different DMUs in cases of multiple inputs (Mecit and Alp, 2013). Therefore, this particular DEA model appears to be appropriate to provide an efficiency measure for InfoSec in business processes.

2.4 Previous Research

Data envelopment analysis is a popular tool in management analysis to evaluate efficiency and performance. It is normally used to evaluate DMUs that represent businesses or operations in, for instance, mass productions or logistics (Arunyanart, Ohmori and Yoshimoto, 2015; da Silva, Marins, Tamura and Dias, 2017; Zheng and Park, 2016). Like DEA, InfoSec that includes human factors is a thoroughly researched area (e.g. Hougbo and Hounsou, 2015; Lundgren and Möller, 2019; Nyman and Große, 2019; Zalewski et al., 2014). In the area of business processes, research has focussed on the development of models for InfoSec risk analyses (e.g. Hariyanti et al, 2018). For example, InfoSec requirements are used to indicate vulnerabilities in business processes (Taubenberger et al., 2013). Taubenberger and Jürjens (2008) have proposed a method for identifying InfoSec risk events within business processes. However, there is a lack of methods for comparison between process settings, which can improve business process development to include a certain level of InfoSec. Moreover, studies have not yet investigated how DEA can provide a tool for evaluating InfoSec among business processes. Thus, this paper aims to address this gap.

3 METHOD

This paper provides a model that can assist with benchmarking InfoSec in business processes.

First, this study presents a mathematical model that is based on DEA. The development of the DEA model departed from the preceding literature review and analyses of business process models using BPMN (see Figure 2 for an example of a business process model). Factors in the processes that particularly relate to human interaction with information, and can

thus affect InfoSec, have been included in the model. Such factors appear as inputs in the DEA. Departing from the review of human factors in literature (see Section 2) and various business process models (for example, see Figure 2), this study restricts the DEA model to the following inputs, which are considered to affect confidentiality, integrity and availability.

- Data storage and access
- Automatic and manual processes
- Change in information form
- Passwords

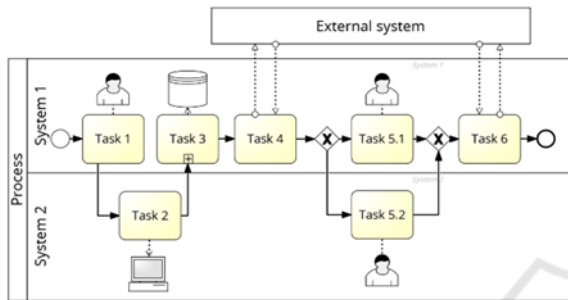


Figure 2: Example business model using BPMN.

These inputs can be evaluated for the degree to which they are satisfied. Even though such inputs can be equally fulfilled, they can have different impacts on the InfoSec of the process. For instance, passwords can vary in strength, or organisations might apply specific requirements for password strength in different processes. Furthermore, the classification of information in processes can vary from highly confidential to public. Hence, each input in the DEA model must reflect specific considerations about these aspects, as they change the efficiency according to the InfoSec of a particular process. One way to handle such variation is to weight the inputs.

Second, an example implementation of this model demonstrates its usability. A comparison of three processes – one IDMU and two fictive DMUs – illustrates the evaluation of InfoSec in business processes from a human factor perspective. Whereas the IDMU mirrors the ideal level of InfoSec, DMU 1 and DMU 2 exemplify possible implementations.

To illustrate the usage of the proposed model for evaluating business process settings, all values for DMU 1 and DMU 2 were randomly chosen in Excel by the function RANDBETWEEN. This function returns a random integer number in an interval, which was predefined to exemplify the method (see 4.1). The general scenario in this study has been set as follows:

- Maximal 12 people who have access,
- Maximal 30 manual processing of data,

- Twenty data transfers during which information can change its form,
- Five events where passwords could be required

Whereas the IDMU reflects the perfect process, which is defined by the predefined inputs that matches the efficiency score of 1.0, DMU 1 and DMU 2 provide a possible set of variables that could relate to a business process in any organisation.

4 MEASURING INFOSEC

4.1 The DEA Model

This section details the DEA model that this study applies to assess InfoSec in business processes. The resulting efficiency score can be used to not only measure InfoSec but also benchmark business processes within and among organisations.

The model seeks the maximum efficiency through the sum of the output weights multiplied by the output values (see Equation 1).

$$\max \theta = \sum_{r=1}^s u_r y_{r0} \tag{1}$$

$$\text{s.t.} \sum_{i=1}^m v_i x_{i0} = 1 \quad i = 1, \dots, m; \tag{2}$$

$$\sum_{r=1}^s u_r y_{rj} - \sum_{i=1}^m v_i x_{ij} \leq 0 \quad j = 1, \dots, n; \tag{3}$$

$$A_i \leq \frac{v_i}{v_k} \leq B_k \quad i < k, i, k = 1, \dots, m; \tag{4}$$

$$a_r \leq \frac{u_r}{u_t} \leq b_t \quad r < t, r, t = 1, \dots, s; \tag{5}$$

$$x' = 1 - x \tag{6}$$

$$x' = 0.8 * (x) + 0.1 \tag{7}$$

θ : efficiency,
 u : weight to the output y ,
 v : weight to the input x
 B_k, b_t : upper boundaries for the weights
 A_i, a_r : lower boundaries for the weights

Equations 2 to 5 specify the constraints of the DEA model. The sum of the weighted inputs must be equal to one, and the difference between the sums of the weighted outputs and inputs must be greater than or equal to zero, according to Equations 2 and 3, respectively. Equations 4 and 5 set the boundaries for the weight restrictions (Arunyanart et al., 2015; da Silva et al., 2017; Lertworasirikul, Fang, Nuttle and Joines, 2003; Opricović and Tzeng, 2008; Seiford and Zhu, 1999; Zheng and Park, 2016).

In the case that some inputs are negative, and others are positive, the negative ones must be pre-processed to fit the model. To this end, the inverse is calculated with Equation 6. Moreover, it can be assumed that total InfoSec can hardly be achieved, and it probably cannot be lower than zero. Therefore, input values should be normalised within an interval that appropriately reflects these considerations. Therefore, Equation 7 displays a determined interval. This study defines the interval between 0.1 and 0.9, which adopts the previous reflections and leaves room for InfoSec developments in both directions.

4.2 InfoSec Efficiency in Processes

This section presents an example implementation of the DEA model to demonstrate its usability for measuring InfoSec efficiency in business processes. Three processes – one IDMU and two fictive DMUs – exemplify evaluation of InfoSec that involves human factors. The following example primarily aims to explain the principles of the proposed model and thereby to encourage a discussion of this measure.

The inputs of the IDMU departed from the general scenario, and their weights emerged from the brief review of recommendations for good InfoSec in literature (see e.g. Gonzalez and Sawicka, 2002; Nyman and Große, 2019; Venegas, 2007). As mentioned, the values for DMU 1 and DMU 2 were randomly chosen, to exemplify a possible scenario. Table 1 displays the values for the three processes.

Table 1: Input values for the DMUs.

Input	DMU 1	DMU 2	IDMU
Number of people who have access to processed information (EA)	10 of 12	12 of 12	5 of 12
Manual processing (MP)	23 of 30	8 of 30	5 of 30
Changes of information form (IC)	10 of 20	7 of 20	5 of 20
Password required (PW)	3 of 5	2 of 5	5 of 5

The minimum for employee access (EA) is set to allow five persons to have access to the information within the business process. The minimum times for manual information processing (MP) was also set to five during the process. The general scenario transfers information 20 times; thus, the form of information can change. Information sometimes needs change, such as when information appears first within an e-mail and must be transferred into an enterprise resource planning system. Hence, the minimum of five changes with respect to the form of information (IC) is set to be optimal. In contrast, a maximum of

five process events in which passwords (PW) can be required has been determined as optimal in the IDMU.

As the description of the inputs reveals, the first three negatively impact InfoSec, while the latter has a positive effect. Therefore, the inverses of the former three inputs must be calculated, which return the effects that support the maximisation model regarding InfoSec. Table 2 presents the processed input values for the DEA model.

Table 2: Input values for DMUs after inverse calculation.

Input	DMU 1	DMU 2	IDMU
EA	16,66%	0%	58,33%
MP	23,33%	73,33%	83,33%
IC	50%	65%	75%
PW	60%	40%	100%

In the final step of the DEA model, the values are normalised to enable the model to return an efficiency measure, which can be used to evaluate InfoSec with regard to human factors in business processes.

Table 3 presents the final input values for calculating the InfoSec efficiency measure. The values are normalised with Equation 7.

Table 3: Input values for the DMUs after normalisation.

Input	DMU 1	DMU 2	IDMU
EA	0,76667	0,9	0,4333
MP	0,71333	0,3133	0,2333
IC	0,5	0,38	0,3
PW	0,42	0,58	0,1

The example in this study applies the following weight restriction: no input weight can be more than double another input weight.

Table 4 displays the results from the implementation of the proposed DEA model on three variants of a fictive business process. The displayed efficiency scores indicate that the IDMU is approximately twice as efficient as DMU 1 and DMU 2.

Table 4: Efficiency scores for InfoSec in the DMUs.

DMU	Efficiency according to InfoSec
IDMU	1.000
DMU1	0.491
DMU2	0.558

Since DMU 2 yields a higher efficiency score, this process can be considered to incorporate superior InfoSec. In particular, the process involves a lower number of both manual processing of information and

changes of its form. The differences in the inputs regarding password implementation and employee access to the information within the processes were relatively small between DMU 1 and DMU 2. Therefore, even though DMU 1 slightly outperformed DMU 2 in these inputs, this small advantage could not regain the losses of efficiency that relate to the other two. Both DMUs obtained a noticeably lower efficiency compared to the ideal process, which illustrates the importance of enhancing each aspect that affects InfoSec in business processes that relate to both technical and human aspects.

5 DISCUSSION

5.1 Treatment of the Model

The proposed model is a tool for evaluating InfoSec in business processes that include information flows and interaction between employees and the processed information. However, it is important to understand that the efficiency measure in this model indicates how one DMU compares to the others that the model includes. Thus, the scores in Table 4 reflect the relative performance of the processes regarding the efficiency of InfoSec. For example, the IDMU yields an efficiency score of 1.0 according to InfoSec. This score suggests that the IDMU is the ideal process compared to the others. In other process settings, this IDMU may perform with less success and yield other scores. Therefore, the efficiency scores of this model are not easily transferable; instead, all processes must be included in the model to compare their efficiency.

Moreover, it is advisable to notice that InfoSec can hardly be absolute. The proposed model seeks to account for this aspect through normalisation of the input values into a predefined interval. For the scope of this study, the DEA provides a proper method because it facilitates an individual assessment of each input. In addition, the DEA model allows for the inclusion of a larger number of inputs beyond the four in the example, which can expand the implementation.

5.2 Critical Discussion of the Approach

Although the proposed model provides an appealing method to assess InfoSec that interrelates to human interaction with information in business processes, there are some concerns with the current state of the approach, which we intend to address in future work.

First, the demonstration of the method in this study includes four inputs in two fictive processes.

Hence, a further improvement of the proposed model must include a larger number of factors that can affect InfoSec, particularly with regard to human interaction with information. In addition, an examination of a larger number of business process models and real implementations could be used to improve the comprehensiveness and validity of the method.

Second, the BPMN is viewed as tool to support InfoSec assessments because it enables the visualisation of information processing and the inclusion of privacy requirements in business process models (Bartolini, Calabro and Marchetti, 2019). In this study, BPMN has been a useful tool to identify events that can involve human interaction with information. Depending on the granularity of such business process models, they can facilitate InfoSec risk analysis (Hariyanti et al, 2018; Taubenberger et al., 2013; Taubenberger and Jürjens, 2008). However, further research is needed to substantiate a systematic transfer of identified events into the DEA model as well as the inclusion of privacy aspects in the method.

Third, associated with the previous concern, the evaluation of the proposed model in this study applies a general scenario and randomly generated inputs to exemplify two processes. Further developments need to include real examples of business process settings for proper method evaluation and improvement. As indicated, regular process and risk assessment could enhance the method, for example to determine the upper and lower boundaries in the DEA model with respect to the desired level of InfoSec in a particular organisation.

Although the proposed DEA model provides a method to benchmark InfoSec in business processes, the inputs that substantiate the model must be subject to careful in-depth assessment and monitoring in order to adopt the method to particular settings. Therefore, further research could study appropriate inputs and methods to attribute weights and boundaries, which also could address benchmarking and comparability between different businesses.

5.3 Implications for the InfoSec Field

In practice, a detailed modelling of selected business processes should precede any implementation of the proposed DEA model. The initial investigation for this study as well as the previous discussions recommend the usage of BPMN for this task because it provides elements to model the interrelations, flows and interactions during business processes as well as the interrelated InfoSec requirements (Bartolini, Calabro and Marchetti, 2019).

A comprehensive business process model facilitates an analysis of weaknesses and strengths regarding InfoSec as previous research has encouraged (Hariyanti et al, 2018; Taubenberger et al., 2013; Taubenberger and Jürjens, 2008). Such analysis can reveal areas for improvement and risk reduction. In departing from these areas, an implementation of the DEA model in practice can focus on several human aspects of InfoSec even besides those that this study has applied (e.g. Hougbo and Hounsou, 2015; Lundgren and Möller, 2019; Nyman and Große, 2019; Zalewski et al., 2014). All aspects that can be measured can fit in the DEA model as either input or output. Depending on a particular organisation and its processes, various inputs can be considered and selected for closer evaluation, whereas other organisations may value similar inputs in a unique way.

However, each input must be carefully defined for both types of processes – the ideal one and those that are subject to the evaluation. To improve such definition, each input should be evaluated from an InfoSec perspective. One option is to multiply an input value by a factor that reflects the potential of this particular input to affect the InfoSec in this business process. All input values ideally derive from a regular assessment of the business processes. An implementation of the DEA model can then use proper values in the calculations. This approach strengthens the quality of the benchmarking with the aid of the InfoSec efficiency measure.

This study suggests that future research should include a larger variety of both technical and human aspects of InfoSec in the DEA model, especially regarding issues that relate to the General Data Protection Regulation (GDPR), such as traceability and privacy. In addition, further research could investigate how organisations select, assess and value inputs for the model in order to refine the proposed method and the resulting InfoSec efficiency measure.

6 CONCLUSIONS

Measuring InfoSec in organisational business processes is challenging because it involves both technical and human factors. This study proposes a novel approach to assess InfoSec among business processes in organisations. The new method facilitates the identification of internal threats and further provides an InfoSec efficiency measure to compare process models and implementations. Assessments of InfoSec in organisations commonly apply techniques and tools that target external threats

or potential attackers. Accordingly, internal threats are acknowledged but not regularly included. The suggested approach therefore integrates DEA in evaluations of business process models during which human interaction occurs with processed information. An example application of the proposed approach has demonstrated its usefulness for measuring InfoSec. This study thus contributes a tool for comparing InfoSec among business processes and a desired level of InfoSec, which also facilitates the assessment of improvements within business processes. The proposed DEA model for calculating an InfoSec efficiency measure for a portfolio of business models provides a valuable tool to organisational efforts to enhance InfoSec in business processes, before implementation as well as during operation.

REFERENCES

- AlFayyadh, B., Thorsheim, P., Jøsang, A., and Klevjer, H. (2012). Improving Usability of Password Management with Standardized Password Policies. In: Rosenberger, C., and Achemlal, M. (eds) *Proceedings of the 7th Conference on Network and Information Systems Security*, 38–45.
- Arunyanart, S., Ohmori, S., and Yoshimoto, K. (2015). Pairwise Comparison for Weight Restriction in DEA/ARI. *International Journal of Japan Association for Management Systems*, 7(1), 53–60.
- Badenhorst, J. A., Maurer, C., and Brevis-Landsberg, T. (2013). Developing measures for the evaluation of information flow efficiency in supply chains. *Journal of Transport and Supply Chain Management*, 7(1), 13.
- Bartolini, C., Calabro, A., & Marchetti, E. (2019). Enhancing Business Process Modelling with Data Protection Compliance: An Ontology-based Proposal. In: *Proceedings of the 5th International Conference on Information Systems Security and Privacy*, 421–428.
- Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-based Beliefs and Information Security Awareness. *Management Information Systems Quarterly*, 34(3), 523–548.
- Charnes, A., Cooper, W. W. and Rhodes, E. (1978). Measuring the efficiency of decision making units. *European Journal of Operation Research*, 2, 429–444.
- Cohen, F. (2011). How do we measure security? *INCOSE Insight* 14(2), 30–32.
- da Silva, A. F., Marins, F. A. S., Tamura, P. M., and Dias, E. X. (2017). Bi-Objective Multiple Criteria Data Envelopment Analysis combined with the Overall Equipment Effectiveness: An application in an automotive company. *Journal of Cleaner Production*, 157, 278–288.
- Garza-Reyes, J. A., Torres Romero, J., Govindan, K., Cherrafi, A., and Ramanathan, U. (2018). A PDCA-based approach to Environmental Value Stream

- Mapping (E-VSM). *Journal of Cleaner Production*, 180, 335–348.
- Geiger, M., Harrer, S., Lenhard, J., and Wirtz, G. (2018). BPMN 2.0: The state of support and implementation. *Future Generation Computer Systems*, 80, 250–262.
- Gonzalez, J. J., and Sawicka, A. (2002). A Framework for Human Factors in Information Security. In: *Proceedings of WSEAS International Conference on Information Security*.
- Große, C. (2016). *Towards an Integrated Framework for Quality and Information Security Management in Small Companies*. Luleå University of Technology.
- Hariyanti, E., Djunaidy, A. and Siahaan, D.O. (2018): A Conceptual Model for Information Security Risk Considering Business Process Perspective. In: *4th International Conference on Science and Technology*. IEEE, pp. 1–6.
- Houngbo, P. J. and Hounsou, J. T. (2015). Measuring Information Security: Understanding and Selecting Appropriate Metrics. *International Journal of Computer Science and Security*, 9(2), 108-120.
- Hwang, I., and Cha, O. (2018). Examining technostress creators and role stress as potential threats to employees' information security compliance. *Computers in Human Behavior*, 81, 282–293.
- International Organization for Standardization (ISO) (2013). ISO/IEC 19510:2013. Information technology — Object Management Group Business Process Model and Notation.
- International Organization for Standardization (ISO) (2018). ISO/IEC 27000:2018. Information technology — Security techniques — Information security management systems — Overview and vocabulary.
- Komanduri, S., Shay, R., Kelley, P. G., Mazurek, M. L., Bauer, L., Christin, N., Cranor, L. F., and Egelman, S. (2011). Of passwords and people: Measuring the effect of password-composition policies. *Proceedings of the 2011 Annual Conference on Human Factors in Computing Systems*, 2595.
- Lawrence, G. W., Kehoe, W. R., Rieger, O. Y., Walters, W. H. and Kenney, A. R. (2000). *Risk management of digital information: A file format investigation*. Washington, D.C: Council on Library and Information Resources.
- Laybats, C., and Tredinnick, L. (2016). Information security. *Business Information Review*, 33(2), 76–80.
- Lertworasirikul, S., Fang, S.-C., Nuttle, H. L. W. and Joines, J. A. (2003). Fuzzy BCC Model for Data Envelopment Analysis. *Fuzzy Optimization and Decision Making*, 2(4), 337–358.
- Lundgren, B., and Möller, N. (2019). Defining Information Security. *Science and Engineering Ethics*, 25(2), 419–441.
- Mecit, E. D. and Alp, I. (2013). A new proposed model of restricted data envelopment analysis by correlation coefficients. *Applied Mathematical Modelling* 37, 3407-3425.
- Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., and Giannakopoulos, G. (2014). The Human Factor of Information Security: Unintentional Damage Perspective. *Procedia - Social and Behavioral Sciences*, 147, 424–428.
- Mitrovic, P. (2005). *Handbok i IT-säkerhet* (4th ed.). Sundbyberg: Pagina Förlags AB.
- Nyman, M. and Große, C. (2019). Are You Ready When It Counts? IT Consulting Firm's Information Security Incident Management. In: *Proceedings of the 5th International Conference on Information Systems Security and Privacy*, 26-37.
- Opricović, S., and Tzeng, G.-H. (2008). A comparative analysis of the DEA-CCR model and the VIKOR method. *Yugoslav Journal of Operations Research*, 18.
- Paliszkievicz, J. (2019). Information Security Policy Compliance: Leadership and Trust. *Journal of Computer Information Systems*, 59(3), 211–217.
- Pereira T. and Santos H. (2015). Insider Threats: The Major Challenge to Security Risk Management. In: Tryfonas, T., Askoxylakis, I. (eds) *Human Aspects of Information Security, Privacy, and Trust 2015. Lecture Notes in Computer Science*, vol 9190. Springer, Cham.
- Seiford, L. M., and Zhu, J. (1999). An investigation of returns to scale in data envelopment analysis. *Omega*, 27(1), 1–11.
- Stolfo, S., Bellovin, S. M. and Evans, D. (2011). Measuring Security. In: Varadharajan, V. and Cohen, F. (eds) *On the Horizon. IEEE Security & Privacy* 5/6 2011, 60-65
- Taubenberger, S. and Jürjens, J. (2008). IT Security Risk Analysis based on Business Process Models enhanced with Security Requirements. In: *Proceedings of the Workshop on Modeling Security 2008 at International Conference on Model Driven Engineering Languages and Systems*. Paper 14.
- Taubenberger, S., Jurjens, J., Yu, Y. and Nuseibeh, B. (2013). Resolving vulnerability identification errors using security requirements on business process models. *Information Management and Computer Security*, 21(3), 202–223.
- Venegas, C. (2007). *Flow in the Office—Implementing and sustaining Lean improvements*. CRC Press.
- Vroom, C., and von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security*, 23(3), 191–198.
- Wang, Y.-M., and Luo, Y. (2006). DEA efficiency assessment using ideal and anti-ideal decision making units. *Applied Mathematics and Computation*, 173(2), 902–915.
- Wood, C. C. (1983). Effective information system security with password controls. *Computers & Security*, 2(1), 5–10.
- Zalewski, J., Drager, S., McKeever, W. and Kornecki, A.J. (2014): Measuring Security. A Challenge for the Generation. In: *Federated Conference on Computer Science and Information Systems*. pp. 131–140.
- Zheng, X. B. and Park, N. K. (2016). A Study on the Efficiency of Container Terminals in Korea and China. *The Asian Journal of Shipping and Logistics*, 32(4), 213–220.
- Zhu, J. (2014). *Quantitative models for performance evaluation and benchmarking: Data Envelopment Analysis with Spreadsheets*. 3rd ed. Springer International Publishing.