Risk variance: Towards a definition of varying outcomes of IT security risk assessment

Sebastian Kurowski[1], Christian H. Schunck[2]

Abstract: Assessing IT-security risks in order to achieve adequate and efficient protection measures has become the core idea of various industry practices and regulatory frameworks in the last five years. Some research however suggests that the practice of assessing IT security risks may be subject to varying outcomes depending on personal, situational and contextual factors. In this contribution we first provide a definition of risk variance as the variation of risk assessment outcomes due to individual traits, the processual environment, the domain of the assessor, and possibly the target of the assessed risk. We then present the outcome of an interview series with 9 decision makers from different companies that aimed at discussing whether risk variance is an issue in their risk assessment procedures. Finally, we elaborate on the generalizability of the concept of risk variance, despite the low sample size in light of varying risk assessment procedures discussed in the interviews. We find that risk variance could be a general problem of current risk assessment procedures.

Keywords: Risk Analysis, Risk Assessment, Risk Management, IT-Security, Information Security

1 Introduction

Risk analysis has become an important cornerstone of information security management. For instance, the EU General Data Protection Regulation (GDPR) requires security measures to be adequate in light of the risk for the data subjects rights and liberties (Article 32, paragraph 1 and article 24, paragraph 1, GDPR). Industrial Frameworks such as the VDA Information Security Assessment (ISA) [VD15] require a security level and thus risk associated characterization of security measures. These are just two example of frameworks that have shifted towards a risk-based approach, putting the justifiability of security measures at their core. This development seems reasonable, since managing information security around assessed information security risks allows organizations not just to choose the right security measures, but to align their budgets accordingly, and to

[1] Fraunhofer IAO, Fraunhofer Institute for Industrial Engineering IAO, Team identity management, Nobelstr. 12, Stuttgart, 70569, sebastian.kurowski@iao.fraunhofer.de

[2] Fraunhofer IAO, Fraunhofer Institute for Industrial Engineering IAO, Team identity management, Nobelstr. 12, Stuttgart, 70569, christian.schunck@iao.fraunhofer.de https://orcid.org/0000-0002-7917-8180

The research presented in this paper was partially funded by the federal ministry for economic affairs and climate action under grant no. 01MT19006B and partially funded by the Zero Outage Industry Standard Ltd.

doi:18.18420/OID2022-08

have reasonable justification if incidents happen despite taken efforts. However, these advantages can only materialize, if the assessment of risks is reliable and factual. Reasonable justifications can only stand if the risk has been regarded beyond possible doubt. The optimal budget can only be determined if risks have been assessed without any biases. In the largely positivistic research area of IT- and information security the factuality of risk assessments is often assumed implicitly. Yet Baskerville drew an argument for the interpretivistic nature of risk assessments [Ba91], indicating that these may be biased by the person interpreting the risk. Additionally, Luhmann [Lu90] provides an argument for the subjectivity of risks by arguing that a risk is an anticipation of observed threats. This can also incidcate that the assessment of risks may not only be subject to individual, subjective traits but also to factors surrounding the anticipation of a risk and the observation of a threat. Finally, the dissertation by Mersinas [Me17] shows that decision making and attitude of security deciders can be influenced by risk aversion and affinity.

This raises the question: Can risk assessments vary based on non-risk related traits?

In this contribution we coin the term risk variance as varying outcomes of risk assessments. We provide the results of semi-structed interviews with nine decision makers from the IT and information security domain in different organizations on the existence of variance in risk assessments. We then discuss the findings along the existing body of knowledge on influencing factors of decision making and arrive at a definition of risk variance. We also discuss how general the problem of risk variance, and the identified factors could be. The following section provides a first characterization of what could possibly characterize risk variance, followed by a brief discussion of the current state of the art of risk assessments.

2 State of the Art

2.1 Variation and biases in security decision making

Some publications discovered biases in security decision making. Hyeun-Suk et al. [Hy12] showed that security decision makers would tend to assess other companies as more vulnerable than their own company. Mersinas [Me17] showed that decision makers indicate subjective affinity or aversion towards certain risk scenarios. Still, the subjectivity of organizational analyses, organizational decision-making, and thus also risk assessment is a rare research subject in information and IT security research.

However, extensive research exists from the field of psychology, sociology and economics. The research of Kahneman and Tversky [KT79] shows that individuals can indicate affinity or aversion towards specific risk scenarios, which matches the findings by Mersinas [Me17]. Nosofsky [No83] and later Benjamin et al. [Be09] showed that criterion selections can change based on the presentation of those criterions (criterion noise). E.g. the number of criterions can increase criterion noise, while providing overviews can decrease it. Gilboa and Schmeidler [GS89] showed that subjects tend to regard known scenarios as more significant than unknown scenarios. And finally, Hermand et al. [He03] find that the target that a risk applies to (risk target) influences the significance of that risk for the assessing individual. They showed that risks that apply to strangers are perceived more likely, than those that apply to the assessors. This shows that while there is few existing evidence for varying outcomes of decision-making processes in IT- or information security, there is a large body of knowledge on possible individual, situational, presentational (i.e. criterion noise), and contextual influences, that may as well apply to IT- or information security.

2.2 Variation in risk assessment approaches

These factors, however, do not play any role in current risk assessment approaches. Good practices and norms such as ISO/IEC 27005:2018 [Is18], OCTAVE, OCTAVE FORTE [AD02], ITU X.1208 , NIST SP 800-122 , BSI-Standard 200-3, factor analysis of information risk (FAIR), or the French "expression des besoins et identification des objectivs de sécurité" (EBIOS) do not take assessor traits, situational traits, or any other influencing factors into account. The only existing norm that considers its organization surrounding is NIST SP 800-30, which requires risk assessments to be structured along the organization's hierarchy. Peer reviewed literature on risk assessments on the other hand largely considers automation approaches, over variation minimization. Zhang and Rao use neural networks [Zr20] for risk assessments, Shakibazad and Rashidi [Sh20] build upon pre-assessed vulnerability scores which are assumed to be objective, Riesco and Villagra build assessments on large semantic networks [RV19], Rios et al. use attack trees [Ri20], and James [Ja19] derives risk assessments based on deterministic finite automation. None of these approaches take the variability of inputs or the variable interpretation of outputs into account. But even in non- or semi-automated approaches, assessment procedures reducing or avoiding possible variances do not play a role. Teng et al. [Te20] employ an analytical hierarchy process (AHP) [Sa88] in order to weigh different risks. While this could potentially decrease criterion noise, it does not weigh on the other possible influencing factors. Sektas-Bilusisch et al. [Se20] combine focus groups with a formal model in order to assess risks. However, they as well do not take any possible variations in account. This shows that the variation of risk outcomes based on individual, situational, presentational, and contextual cues is not yet considered within industry practices, norms, or research.

3 On the relevance of risk variance

Since no direct evidence of risk variance could be obtained from existing literature, yet the existence of this problem seemed to be plausible in light of the body of knowledge of other research domains, we conducted an interview series with nine different decision makers from nine different organizations.

3.1 Sampling and Data Capturing

The interviews aimed at verifying or falsifying the existence of risk variance in the IT- and information security risk assessment processes of these companies. Additionally, details on how risks are conducted, which norms are used, what role security plays within the organization, and if risk variance was observed, how the organization mitigates this variance were sought. These interview aims provide both exploratory and confirmatory research questions. Therefore, a semi-structured interview methodology was used [My09] as it allowed the interviewers to deviate from the question script in order to further explore the responses of interviewees. The interviews were conducted as part of a funded project by an association for IT availability. This allowed for the acquisition of interview partners from the members of this association. While the thematic frame of the association (along with a small sample size) may hinder the generalizability of these findings, we were still able to acquire interviewees from different functions including information security, quality management, sales and executive roles. Interviews were conducted by two interviewers. Given that interviewees consented to recording, all interviews were recorded for later analysis and deleted after the analysis was finished. No interviewee objected to the interview being recorded. A third researcher transcribed the interviews, which were then used for analysis.

3.2 Data analysis

Due to the explorative properties of semi-structured interviews, one of the main tasks of the analysis methodology was to reduce the possible variety of statements without losing too much information. Qualitative content analysis (QCA) was chosen for this purpose [EK08][Sc19]. QCA provides for interview transcripts to be analysed with a thematic framework of main themes and sub-themes. The use of code systems for analysis within the thematic framework is not obligatory. Therefore, code systems were not used in the analysis of the interviews. Although these represent a considerable reduction of the data [GL13], an ex-ante elaboration of code systems would get in the way of the explorative character of the data. An elaboration of codes during the analysis, as used for example in grounded theory based analysis approaches [GS71][HJ03] also did not seem profitable, as an elaboration of explanatory substantive and general theories [Ur09] would go beyond the scope of this publication. Furthermore, due to the number of interview partners (n=9), no value was seen in quantitative analysis, which ultimately led to the decision not to use code systems. The thematic framework was used by two researchers working independently to interpret the transcribed responses. These interpretations were then checked for agreement by both researchers. Discrepancies were resolved in a meta-interpretation. This meta-interpretation was finally used for a narrative summary, similar to a narrative review of literature [Ja16]. The thematic framework used for the analysis is presented in the Appendix. This represents the respective main topics on which the analysis is based. For example, risk analysis questions should be considered in terms of their degree of systematisation (standards used, use of standards, risk factors considered, weighting/measurement of risk, abstract description of approach). Analysis-initiating factors should be distinguished in terms of regular and irregular factors. The regularity of the analysis was considered exclusively in terms of the period after which an analysis is repeated. Influences on monetary planning and reserves were considered in terms of their existence, the nature of the influence and the monetary aspects influenced. In contrast, purposes of the risk analysis that go beyond this were not to be explored in greater depth. The influence of risk analysis on the company was additionally regarded by the thematic framework. The monetary influence was in the foreground, since this could play a supporting role for the concept of efficiency under the assumption that entrepreneurial action can be reduced to the exchange of monetarily measurable resources. However, additional purposes of risk analysis can indicate its value for the company's success. The occurrence of risk variance was analysed with regard to its existence in principle and possible reasons for it. If risk variances occur in the company, possible limiting countermeasures were recorded. If none occurred, possible preventive countermeasures were considered. However, this case did not occur with any of the interview partners. Finally, the analysis of the demographic questions aimed to analyse the current perspective on the company, the professional proximity to risk analyses, relevant previous experience and the relevance of the topic of information security for the organisation itself, both in absolute terms and in relation to other important (open) topics such as customer satisfaction, or shareholder value. In the course of the analysis, it became apparent that interviewee 8 could not give any organisation-specific answers due to his role as a security consultant. Since the statements therefore referred to his general view, but not to a specific company, the answers were excluded from the development of the meta-interpretation. This results in an effective sample of (n=8).

3.3 Findings

Tab. 2 shows that all interviewees claimed that they have observed risk variance in their risk assessment outcome. This is especially interesting, as the standardization of the risk assessment process varies from standardized according to international norms, standardized according to company specific processes, semi-standardized with checklists and templates to ad-hoc improvised assessment processes. Obviously the systematicity of assessments does not mitigate risk variance sufficiently.

R.V.[*]	Impact as..	Probability as..	Risk aspects	Standardization
✓	Business Impact	Quantitative	B, S, O	ISO 27k process
✓	Financial Impact	No information	S, P, Fi, Pr	No information

R.V.*	Impact as..	Probability as..	Risk aspects	Standardization
✓	Financial Impact if possible	Semi-Quantitative / Quantitative if possible	S	Standardized company specific process
✓	Expert Opinion / Data if possible	Quantitative based on expert opinion / Data if possible	S, B, O, Pr, Prod, Ma, Qu, IT	Standardized company specific process
✓	Qualitative	Qualitative	IT, B	Standardized company specific process
✓	Customer-depending	Customer-depending	App	Customer depending
✓	Liability	No information	IT, Fi	Improvised
✓	Financial	Qualitative based on expert opinion	BC	Semi-standardized

* Risk Variance, ✓ Risk variance observed, B = Business Risk, S = Security Risk, O = Organizational Integration, P = Privacy Risk, Fi = Financial Risk, Pr = Price Risk, Se = Service Risk, Pr = Provisioning Risk, Prod = Production Risk, Ma = Marketing Risk, Qu = Quality Risk, IT = IT Risk, App = Application Downtime, BC = Business Continuity

Tab. 1 Observed risk variance and risk assessment characteristics mentioned by the interviewees

The same holds for the role of quantification. Some researchers, e.g. [Zu20] sometimes confuse quantification with objectiveness of results. However, our results clearly show that no matter, whether percentage point expert values, ordered non-numerical risk classes, or actual data is used, risk variance always exists within the processes. Finally, there does not seem to be an influence between the broadness of considered risk aspects. Whether risk assessments include the identification of consequences to, or influences from application downtime only, or multiple different aspects within the company, risk variance is always observed.

The factors which interviewees saw as reasons for the varying risk assessments however included risk affinity or aversion, knowledge of the domain, understanding of psychology, empathy, professional background, domain of work, contextual understanding, personality, and the situation of decision-making. Surprisingly, the professional domain was mentioned as a reason for risk variance by three different interviewees. One interviewee mentioned that IT security people might have a focus on exploits but not on topics like emergency crisis management or business continuity. Other interviewees stressed the different views between Chief Financial Officers (CFO) and Chief Information Security Officers (CISO) stressing that the CFO "…didn't see the importance of the security as the [CISO] did.” Instead, the “…CFO was more interested in reducing […] expenses related to what the [CISO] office was demanding.”.

The contextual understanding of a risk scenario was mentioned by two interviewees. One mentioned that a risk assessor can have a different understanding on the services that are provided to customers, how valued the customers are, etc. Another interviewee even mentioned that “sometimes business and sales tell you this is a must win. So, then risk is looked at differently.”.
Knowledge of the domain which is affected by the risk scenario, and an understanding of psychology and empathy in order to “…ask the right questions in the right way and the right times” was mentioned by one interviewee. Interestingly domain knowledge was not mentioned by any other interviewee. However, being able to ask the right questions seems to be related with the situation of decision-making, that has been mentioned by another interviewee. This interviewee claimed that the risks vary based on who it is and also how the decision is made, e.g. after detailed discussions or as an ad-hoc decision. We therefore noted the understanding of psychology and the situation of decision making both as the situation of the risk assessment in Table 3. Finally, individual differences and personality was mentioned by three different interviewees without further details on the specific traits. For instance, one interviewee mentioned that “…managers have very different personalities…”, another one told us that the assessment itself is an “…individual decision.”.

4 Towards a definition of risk variance

The previous section showed that risk variance is an issue with the interviewee’s companies. The observation of risk variance also aligns well with findings on decision-making biases from the fields of psychology, sociology, and economics. However, the reasons given by interviewees for risk variance seem to vary.

Risk affinity or risk aversion is being mentioned by most interviewees. However, it is only mentioned with high, very high, and in one case an unclear assessment of the importance of security in the organization. It is also independent from the IT security focus of these interviewees’ professional experiences. It seems hardly surprising that risk affinity or risk aversion seems to play a role when observing risk variances in organizations with high and very high importance of security. The breadth of possible discussed risk scenarios could be much larger in these companies, unveiling risk affinity or aversion towards certain scenarios more easily. This confirms hypothesis 1.

Interestingly, knowledge of the domain of a risk scenario was only mentioned by one interviewee from a security framework implementation perspective in a company with high importance of security. But if considered together with the contextual understanding of a risk scenario, it spans beyond IT scenarios and is observed with organizations that emphasize security both highly and very highly. It could be that domain-unknowing risk assessors that assess risk scenarios under naïve or overly pessimistic scenarios are more observed with organizations that put more emphasis of risk assessments in more parts of the company, due to the high or very high importance of security. This would also explain why the contextual understanding is also observed by the interviewee with customer representative and management of outsourcing experience. The processual situation in which the risk assessment (situation of risk assessment) is conducted in, is also mentioned together with a high and very high importance of security and by interviewees with management and quality assurance experience. The professionally influenced focus on processes of these interviewees may lead to this observation. The domain of the assessors on the other hand also played a role with medium, high, and customer-focused high importance of security in the companies. It is observed by security management, enterprise architecture, and executive level management professionals. Such professions usually cooperate with various individuals from different domains. The different thought approaches, e.g. of law, psychology, sociology, business management and computer science could yield different conclusions. This however can only be observed by individuals that have worked with different domains as for instance security managers, executive managers, or enterprise architecture managers. All mentioned reasons for risk variance so far seem to be attributable to the interviewees capability of observing them. The variance between the different professional experiences and the importance of security all aligns well with the mentioned reasons. The claim of generalizability thus is almost of esoteric nature. Since we can conclude that: Risk affinity or aversion towards risk scenarios, knowledge of the domain that a risk scenario affects, contextual understanding of the risk scenario, the processual environment of the risk assessment, and the domain of the assessor seem to be general reasons for risk variance. If they are not observable, it currently seems plausible that the reason for this lack of observation may be the lense of the observer and not the non-existence of the reason. Risk variance is therefore to be defined as a variation of outcomes of IT- and information security risk assessments based on individual traits (risk affinity / aversion [KT79][Me17], knowledge of the domain [GS89], contextual understanding of the scenario), the processual environment (presentational cues [Be09][No83], social cues [Lu90]), and the domain of the assessor. Risk target [He03] was the only possible aspect of risk variance that was not mentioned by the interviewees. However, this could also be due to the lack of observability beyond experimental setups and targeted questioning of individuals.

5 Conclusion

This contribution provides insights from an interview series with 9 interviewees on the issue of risk variance. It uses the existing body of knowledge along with the insights from the interviews in order to arrive at a definition of risk variance. It also discussed the possible generalizability of these findings, beyond conceptual or sampling-based generalizability. We found that risk variance is an issue with all interviewees. The reasons for risk variance however vary slightly between the interviewees. Yet, this can be explained by the different lenses of the interview partners. Additionally, the mentioned reasons align well with the body of knowledge on possible influencing factors of decision making under uncertainty. We therefore assume that risk variance is a generalizable issue. The definition provided in this contribution however is not possibly conceptually saturated. Hereby the severity of risk variance is not necessarily depending on the variation between two assessments by the same person. It can be severe however, if compliance goals are not met, due to variations between the assessments conducted by the organization and the assessments conducted by auditing parties, or their subcontractors. Additionally risk variance can implicate that budget decisions made on an educated argument are suddenly biased by individual, situational, and contextual traits. The question on possible mechanisms that contribute to the identified reasons for risk variance therefore is relevant. The identified reasons in this contribution seem to be due to a lack of understanding of scenarios, a lack of contextual understanding, different social cues, presentation, knowledge, and risk affinity / aversion. Except for the social cues, all of these reasons could potentially be founded in the conceptual richness of the term security risk. I.e. the FAIR ontology involves attacker models, economic models, along with IT specific terminology. This richness of concepts could increase the room for interpretation, failing to frame the decision-making biases, and thus arriving at variation of the resulting assessment. If this is true, then an epistemologically founded re-definition of the concepts of risk with the goal to minimize the conceptual richness of the term could indeed help to minimize risk variance. This however is subject to further research.

6 Annex

#	**Question Type**	**Classification**	
		Name	**Description**
Risk assessment procedures in the organization			
1	*Risk assessment procedures in the organizations*	Used Standards	Name of the standards that are used as part of the risk assessment
		Use of Standards	Role that these standards play in the risk assessment (e.g. as a baseline)
		Risk aspects at play	Parts that are considered as related to the IT security risk
		Weight / size of risk	Quantified or Qualified risk values
		Process	Participants, tasks and their execution order
2	*Triggers for risk assessments*	Irregular triggers	Irregular events that result in a (re-)assessment of risks
		Regular triggers	Regularly occuring events that result in a (re-)assessment of risks

#	Question Type	Classification	
		Name	**Description**
3	*Regularity of risk assessments*	Timespan	Regularity of reassessments
4	*Impact of risk assessments on financial aspects in the organization*	Influencing relationship	Is there an influence on any money matters?
		Type of influence on money matters	How are money matters influenced?
		Influenced aspects of money matters	What kind of money matters are influenced?
5	*Impact on other purposes*	Name of Purpose	Name of the purpose for which a risk assessment is used
Risk variances in the risk assessment procedures			
6	*Existence of risk variance*	Existence of Risk Variance	Existence or in the past observed variances of risk assessments
		Reason for Risk Variance	Assumed reasons for varying risk assessments
6a)	*Mitigating risk variance (if risk variance exists)*	Name of Measure	Measure to limit the outcome of varying risk assessments
6b)	*Preventing risk variance (if risk variance does not exist)*	Name of Measure	Measure to avoid the outcome of varying risk assessments
Demographic questions			
9	*Current role and responsibility*	Name of Role	Name of the role
		Information security related tasks	Tasks with relation to security if not implied by the role
10	*Professional experience*	Information security or IT Experience	Experience in years on security/IT or security/IT related topics
11	*Importance of information security*	Relevance of information security	Order of relevance of information security in the organization
		Relativization of information security	Relativization of information security relevance order in light of other topics or personal opinion of the interviewee

7 Bibliography

[AD02] Alberts, C.J., Dorofee, A.: Managing information security risks: the OCTAVE approach. Addison-Wesley Longman Publishing Co., Inc. (2002).

[Ba91] Baskerville, R.: Risk analysis as a source of professional knowledge. Comput. Secur. 10, 8, 749–764 (1991).

[Be09] Benjamin, A.S. et al.: Signal detection with criterion noise: applications to recognition memory. Psychol. Rev. 116, 1, 84 (2009).

[EK08] Elo, S., Kyngäs, H.: The qualitative content analysis process. J. Adv. Nurs. 62, 1, 107–115 (2008).

[GS89] Gilboa, I., Schmeidler, D.: Maxmin expected utility with non-unique prior. J. Math. Econ. 18, 2, 141–153 (1989). https://doi.org/10.1016/0304-4068(89)90018-9.

[GS71] Glaser, B.S., Strauss, A.: A.(1967). The discovery of grounded theory. N. Y. 581–629 (1971).

[GL13] Glaser, J., Laudel, G.: Life with and without coding: Two methods for early-stage data analysis in qualitative research aiming at causal explanations. Forum: Social Qualitative Research, 14 (2). ISSN 1438-5627. (2013).

[He03] Hermand, D. et al.: Risk target: An interactive context factor in risk perception. Risk Anal. 23, 4, 821–828 (2003).

[HJ03] Hughes, J., Jones, S.: Reflections on the use of Grounded Theory in Interpretive Information Systems Research. In: Proceedings of the ECIS 2003 Conference. pp. 1–10 , Naples, Italy (2003).

[Is18] ISO/IEC: Information technology - Security techniques - Information security risk management. ISO/IEC, Geneva, CH (2018).

[Ja16] Jahan, N. et al.: How to conduct a systematic review: a narrative literature review. Cureus. 8, 11, (2016).

[Ja19] James, F.: A Risk Management Framework and A Generalized Attack Automata for IoT based Smart Home Environment. In: 2019 3rd Cyber Security in Networking Conference (CSNet). pp. 86–90 IEEE, Quito, Ecuador (2019). https://doi.org/10.1109/CSNet47905.2019.9108941.

[KT79] Kahneman, D., Tversky, A.: Prospect Theory: An Analysis of Decision under Risk. Econometrica. 47, 2, 263 (1979). https://doi.org/10.2307/1914185.

[Lu90] Luhmann, N.: Technology, environment and social risk: a systems perspective. Organ. Environ. 4, 3, 223–231 (1990).

[Me17] Mersinas, K.: Risk Perception and Attitude in Information Security Decision-making. Royal Holloway, University of London (2017).

[My09] Myers, M.: Qualitative research in business and management. Sage Publications Ltd, London (2009).

[No83] Nosofsky, R.M.: Information integration and the identification of stimulus noise and criterial noise in absolute judgment. J. Exp. Psychol. Hum. Percept. Perform. 9, 2, 299 (1983).

[RV19] Riesco, R., Villagrá, V.A.: Leveraging cyber threat intelligence for a dynamic risk framework. Int. J. Inf. Secur. 18, 6, 715–739 (2019).

[Ri20] Rios, E. et al.: Continuous Quantitative Risk Management in Smart Grids Using Attack Defense Trees. Sensors. 20, 16, 4404 (2020). https://doi.org/10.3390/s20164404.

[Sa88] Saaty, T.L.: What is the analytic hierarchy process? In: Mathematical models for decision support. pp. 109–121 Springer (1988).

[Sc19] Schreier, M. et al.: Qualitative Content Analysis: Conceptualizations and Challenges in Research Practice—Introduction to the FQS Special Issue" Qualitative Content Analysis I". In: Forum Qualitative Sozialforschung/Forum: Qualitative Social Research. (2019).

[Se20] Sektas-Bilusich, D. et al.: A Risk-Based Framework to Inform Prioritisation of Security Investment for Insider Threats. Int. J. Saf. Secur. Eng. 10, 1, 49–57 (2020). https://doi.org/10.18280/ijsse.100107.

[Sh20] Shakibazad, M., Rashidi, A.J.: New method for assets sensitivity calculation and technical risks assessment in the information systems. IET Inf. Secur. 14, 1, 133–145 (2020). https://doi.org/10.1049/iet-ifs.2018.5390.

[Hy12] hyeun-Suk, R. et al.: Unrealistic optimism on information security management. Comput. Secur. 31, 221–232 (2012).

[Te20] Teng, Y. et al.: Algorithm for quickly improving quantitative analysis of risk assessment of large-scale enterprise information systems. In: 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC). pp. 2512–2515 IEEE, Chongqing, China (2020). https://doi.org/10.1109/ITNEC48623.2020.9085010.

[Ur09] Urquhart, C. et al.: Putting the 'theory' back into grounded theory: guidelines for grounded theory studies in information systems: Guidelines for grounded theory studies in information systems. Inf. Syst. J. 20, 4, 357–381 (2009). https://doi.org/10.1111/j.1365-2575.2009.00328.x.

[VD15] VDA: Information Security Assessment. Verband der Automobilindustrie (VDA), Berlin, Deutschland (2015).

[ZR20] Zhang, Y., Rao, Z.: Research on Information Security Evaluation Based on Artificial Neural Network. In: 2020 3rd International Conference on Advanced Electronic Materials, Computers and Software Engineering (AEMCSE). pp. 424–428 IEEE, Shenzhen, China (2020). https://doi.org/10.1109/AEMCSE50948.2020.00098.

[Zu20] Zuo, J. et al.: Comprehensive Information Security Evaluation Model Based on Multi-Level Decomposition Feedback for IoT. Comput. Mater. Contin. 65, 1, 683–704 (2020). https://doi.org/10.32604/cmc.2020.010793.