

Bucharest University of Economic Studies

Business Administration Doctoral School I



PHD THESIS

Presented and publicly supported by the author:

Michael Matthias Naumann

Title of the PhD-Thesis:

**RESEARCH ON IMPROVING THE ASSESSMENT OF
INFORMATION SECURITY MANAGEMENT
MATURITY RELATED TO SUSTAINABILITY RISKS
IN BUSINESS PROCESSES**

PhD supervisor: Prof. univ. Dr. Doru Alexandru Plesea

Bucharest, April 2026

a) Content

TABLE OF CONTENT

ABSTRACT	3
REZUMAT	4
DEDICATION	5
TABLE OF CONTENT	6
LIST OF ABBREVIATIONS	10
LIST OF FIGURES	13
LIST OF TABLES	14
INTRODUCTION	16
1 CURRENT APPROACHES TO THE INFORMATION SECURITY MANAGEMENT SYSTEM AND REQUIREMENTS IN THE CONTEXT OF SUSTAINABLE BUSINESS PROCESSES	21
1.1 Historical Consideration of Information Security Management Systems	21
1.1.1 Information Security Management Systems	23
1.1.2 Standardization of information security	25
1.2 Information Security, Artificial Intelligence and Resilience	26
1.2.1 Artificial Intelligence	27
1.3 Information security in the context of Industry 4.0	36
2 INFORMATION SECURITY MANAGEMENT SYSTEMS AND SUSTAINABILITY	41
2.1 Sustainability and circular economy	41
2.1.1 Sustainability as part of business	41
2.1.2 The concept of the circular economy	44
2.2 Sustainability risks in business processes	46
2.3 Current developments in the field of integrating sustainability with information security management systems	53
3 MEASURING MATURITY IN INFORMATION SECURITY MANAGEMENT SYSTEMS	63
3.1 Maturity models and levels to measure maturity	63
3.2 Standards for measuring information security	68
3.3 Information Security Management System Metrics and Metrics	73
3.3.1 Standards for Security Metrics	73

3.3.2	Standards for measuring maturity in information security	78
4	ANALYSIS OF INFORMATION SECURITY MANAGEMENT SYSTEMS IN THE CONTEXT OF CIRCULAR ECONOMY, SUSTAINABILITY AND CORPORATE SOCIAL RESPONSIBILITY	80
4.1	Analysis of information security in business processes in the context of the circular economy	80
4.1.1	Context of analysis, research framework	80
4.1.2	Objectives of the Research and Research Method	80
4.1.3	Results from the analysis	82
4.2	Analysis of information security in business processes in the context of Industry 5.0	88
4.2.1	Context of analysis, research framework	88
4.2.2	Objectives of the Research Method	89
4.2.3	Results of the study	92
4.3	Analysis of information security in business processes in terms of sustainability and environmental responsibility	96
4.3.1	Context of the analysis and research framework	96
4.3.2	Objectives of the Research Method	96
4.3.3	Results and analysis	102
5	ANALYSIS OF PROCESS MATURITY, COMPLIANCE AND RISKS IN INFORMATION SECURITY MANAGEMENT SYSTEMS	105
5.1	Analysis of process maturity and compliance of information management systems	105
5.1.1	Context of the analysis	105
5.1.2	Objectives of the research and research method	107
5.1.3	Results of the analysis of process maturity and compliance of information management systems	108
5.2	Assessment of the conformity of information security management systems with the requirements of international standards	120
5.2.1	Context of the research	120
5.2.2	Objectives of the research and research method	123
5.2.3	Results of the conformity assessment of information security management systems with the requirements of international standards	126
5.3	Analysis of risks in information security management systems	135

5.3.1	Context of the analysis	135
5.3.2	Objectives of the research and research method	138
5.3.3	Results of the analysis of risks in information security management systems	141
6	ASSESSMENT OF INFORMATION SECURITY AND PROCESS MATURITY IN INFORMATION SECURITY MANAGEMENT SYSTEMS IN COMPANIES	151
6.1	Analysis of current approaches to assessing information security in companies	151
6.1.1	Context of the analysis	151
6.1.2	Research objectives and research method	152
6.1.3	Results of the analysis of current approaches to the assessment of information security	153
6.2	Assessment of process maturity in information security management systems within companies	161
6.2.1	Context of the research	161
6.2.2	Research objectives and research method	163
6.2.3	Results and recommended measures	169
7	IMPROVEMENT POSSIBILITIES FOR MEASURING THE MATURITY OF INFORMATION SECURITY MANAGEMENT SYSTEMS CONSIDERING SUSTAINABILITY	171
7.1	Principles and general aspects of potential improvements in the measurement of maturity	171
7.2	Development of a new key figure „Information Security and Sustainability Index“ for measuring the maturity of information security management systems.....	173
7.2.1	Determining the maturity levels	187
7.3	Assessment of the effects of the proposed key figure for business processes within information security management systems	188
7.3.1	Implementation of the evaluation matrix.....	190
	CONCLUSIONS	196
	BIBLIOGRAPHY	206
	APPENDIX	227
	Appendix 1: Interviewed companies regarding management system risks and audit findings	228
	Appendix 2: Anonymized results with details of Management Systems of audited companies	230

Appendix 3: Survey feedback for new ISSI metric in company	231
Appendix 4: Example calculation matrix in selected company	232
Appendix 5: Calculation matrix for 20 audited companies	244
ANNEXES	249
Annex 1: List of Author's publications	249

b) Keywords

information security management systems, sustainability risks, information security management system maturity, corporate social responsibility, business process maturity

c) Summary

The doctoral thesis addresses the possibilities of improving the assessment of information security management maturity in relation to sustainability risks in business processes. The starting point is the analysis of current approaches to information security management systems and requirements in the context of sustainable business processes. Based on this, information security management systems and sustainability, and the measurement of maturity in information security management systems are discussed in detail. The research continues to focus on the analysis of information security management systems in the context of the circular economy, sustainability, and corporate social responsibility, as well as on analysis of process maturity, compliance and risks in information security management systems. The assessment of information security and process maturity in information security management systems in companies has also been studied. Based on this research's findings and the doctoral candidate's expertise, the emphasis is on achieving maturity in information security management systems, particularly regarding sustainability as a strategic element to enhance corporate performance.

Therefore, an innovative measurement method with a new metric is being developed to identify improvement opportunities for measuring the maturity of information security management systems with a sustainability focus. The proposed measurement method was tested in practice, with data collected from audit results and implementation at a selected company.

As a result of the research, the doctoral candidate offers solutions for implementing the new metric, based on requirements from information security standards combined with environmental, social, and governance requirements. The advantages, limitations, and restrictions of applying the proposed approach, along with potential future development opportunities, are highlighted.

A transparent overview of the current security status of information within business processes, considering the latest requirements and new technologies, and enabled by the collection and use of data across all business and life areas, is essential for competitiveness as well as for the research needs of current business models. To meet both regulatory and economic requirements, additional topics beyond pure IT operations must be considered. These include, in today's context, the issue of sustainability, encompassing environmental, social, and governance aspects. The combination of these two topics as central factors has been gradually addressed.

To answer the research question and to obtain empirical insights, various research approaches were applied. This was further examined by assessing process maturity and compliance within the information security management system, thereby confirming conformity to defined requirements. Studies were conducted, and a key figure for evaluation was developed. This doctoral research initially analyzed the theoretical part, including research on current IT security implementations in relation to sustainability, the identification of risks, the integration of sustainability into Information Security Management Systems, and the measurement of maturity within Information Security Management Systems. The own research contributions were the analysis of information security with regard to the circular economy, sustainability, and ethical aspects, followed by an analysis of process maturity, compliance, and risks in Information Security Management Systems, and an assessment of information security and maturity in companies. The final objective of this doctoral thesis was reached with the development of an improved measurement using a key figure for process maturity, with a focus on information security and sustainability. The following sections provide a detailed summary of the key points and results for each topic.

The analysis of current approaches to information security management systems and requirements in the context of sustainable business processes gave an overview of the current information security standards and its integration into management systems. It showed how changing requirements and increasing protection goals for information are driven by technological developments. It highlights that both innovation and emerging data threats

underscore their strategic importance for companies. Further, it explained the need to adapt business processes and international standards to meet minimum requirements, ensuring that information security measures are comparable and legally compliant. The research showed that new topics related to data processing and artificial intelligence must align with relevant legal regulations and frameworks to help companies adhere to ethical, legal, and technical standards. Furthermore, it examined the relationship between the resilience of business processes and IT systems, with consideration of information security and artificial intelligence. The discussion also covered Industry 4.0 and the networking of systems and machines through the Internet of Things (IoT) as a key technical driver. In this context, the relationship between information security, artificial intelligence, and the maintenance of supply chains in manufacturing and industry has been discussed in detail.

For *Information Security Management Systems and Sustainability* it has been analyzed and identified which dependencies and current implementation approaches for IT security in relation to sustainability exist. For this the analysis of sustainability and the circular economy, showed the importance for companies in terms of economic efficiency, ethics, social responsibility, and competitiveness. Critical topics such as green IT and sustainable cybersecurity were addressed and shown. Information technology has been analyzed with respect to the circular economy's influence on modern companies' digital processes. This framework highlights resource renewal, extensive data sharing, secure communication, and the efficient utilization of robotics and AI. Another segment discusses sustainability risks and adherence to EU standards like the European Sustainability Reporting Standard (ESRs), examining how sustainability is incorporated into IT projects.

It has been demonstrated that recent advances in integrating sustainability with information security management systems are crucial topics that necessitate organizational changes. Additionally, the usage of blockchain technology within the sustainability sector was analyzed and the relevance here to sustainability was shown. Overall it was presented that the benefits of combining sustainability efforts with information security management systems bring improved resource efficiency, reduced risks, cost reductions, and the integration of security protocols.

Measuring maturity in information security management systems involves determining maturity levels and their corresponding characteristics. It has been analyzed that, besides models and standards for assessing overall process maturity, there are also specific models for evaluating maturity in information security. The analysis revealed that maturity can be

evaluated within emerging trends such as Industry 4.0, artificial intelligence, or circular economy requirements. Furthermore, standards related to measuring information security were presented, highlighting both similarities and differences. The doctoral research identified which existing standards and key figures in the information security field address the distinction between processes and maturity levels. It could be shown that different implementations, requirements, and standardization depend on industry or general regulations. This review of current approaches provides a foundation for further research.

Research on the own contributions for this doctoral research was initiated with the *Analysis of Information Security Management Systems in the Context of Circular Economy, Sustainability and Corporate Social Responsibility*. The circular economy and its relationship with digitalization and information security influence, and will continue to influence, the application of the circular economy in business processes. An analysis was conducted to identify which factors are generally important for a circular economy. Using regression methods, it was determined which economic aspects and insights should be considered in the event of potential national-level adaptation. Based on examples of existing circular economies in European countries, it was analyzed that a high level of resource reuse can be achieved, but energy efficiency remains improvable. The integration of IT into the framework of digitalizing production chains, including the automation of Industry 4.0 and 5.0, led to the conclusion that there is significant potential within companies for sustainability and the circular economy. Analyses and surveys conducted by the European Commission demonstrated that the majority of companies have a positive attitude towards digital technology regarding its environmental impact.

It can further be concluded that effective practices of the circular economy in small and medium-sized enterprises can be realized in contrast to large companies within the context of digital transformation, and how this can be evaluated across various industries. Building on this, the topic of Industry 5.0 has been considered as part of industrial transformation. From the perspective of the European Union, the focus is on sustainability for people, the planet, and resilience. The distinction between Industry 4.0, which emphasizes smart factories, sensor technology, and flexible production systems, and the development toward Industry 5.0, which involves direct interaction among humans, machines, and robotics through artificial intelligence, has been highlighted. As resource utilization and cost efficiency become increasingly important in this context, the consideration of sustainability and the circular economy is crucial. New technologies such as Building Information Modeling (BIM) take

into account both information security factors and other non-functional topics, such as climate and environmental impacts. This includes aspects such as durability and safety within the construction industry, which are considered elements of sustainability. From this perspective, Industry 5.0 aims to support the entire lifecycle of buildings, considering resource consumption and the reusability of building materials. Without further digitalization in the construction sector, supported by concepts from the Industry 5.0 model, a sustainable path toward the circular economy and the optimization of recycling can only be achieved to a limited extent.

As an additional area of research, the integration of sustainability topics into defined industries, such as the real estate sector, has shown that these sectors must also support evolving ecological and social requirements through technological advancements. The so-called sustainable real estate development must consider energy efficiency, waste reduction, and the preservation of biological diversity. Furthermore, economic aspects such as cost reduction and competitiveness must be balanced. The topic of information security will play an increasingly important role in areas such as construction, resource calculation, and in later stages of management and building automation. Achieving sustainability goals and cost reduction through the use of advanced technologies such as artificial intelligence or Industry 5.0 can only be successful with ever-increasing protection of digital data and information.

With the *Analysis of Process Maturity, Conformity, and Risks in Information Security Management Systems* it was shown where gaps still occur within companies even after several years of implementing Information Security Management Systems (ISMS), and why these may not be closed or what the obstacles are. It was found that both the execution of regular, e.g., annual routine tasks such as task tracking, correcting audit findings, and employee training are areas where gaps can develop over time due to manual planning or lack of oversight. It could further be shown that the number of topics decreases after the initial years of certification audits, then reaches a certain plateau and remains there. Even after more than ten years, non-conformities were still identified in areas that should be fully managed within the examined companies. Causes for this included technical implementation issues, the need for improved documentation of new processes, and organizational changes. A central issue is also human interaction, as a lack of employee awareness leads to significant risks for data information security. It was found that company size also plays a role. Small and large companies handle management system tasks much more effectively than medium-sized companies. As a conclusion, a set of measures was defined, which aims to increase internal

reviews of information security management systems (ISMS), implement systematic planning of measures, improve awareness, and achieve better oversight of information security objectives through key figures and maturity levels. Further research examined the topic of risks and the implementation of information security in so-called critical infrastructures, such as energy management or water industry companies. Here, a failure of IT-controlled infrastructure would lead to serious problems in the supply of companies and households. In Germany, these companies are therefore subject to proof or certification requirements. These regular checks are carried out through audits by external certifying bodies. The resulting assessments in the form of audit findings provide insights into both the effective implementation of requirements and a comparison with companies in the private sector in relation to regulated critical infrastructure.

During the audits, company employees are interviewed, and conclusions are drawn about implementation based on documents and site inspections. Here as well, an assessment of the different areas of the international standards, such as ISO/IEC 27001, must be considered. The fact that these consist mainly of high-level requirements from your management system is considered more significant than the subsequent measures, which address technical, organizational, personnel, and physical security requirements and specify more concrete procedures. Additionally, operators of critical infrastructure must meet further requirements, for example, for energy supply, according to ISO/IEC 27019. It was also found that most non-conformities in both critical and non-critical companies fall within the technical, organizational, or personnel requirements of the ISO 27001 framework. Furthermore, a higher number of non-conformities was identified across all examined companies in the non-critical and thus less regulated operators. A detailed analysis revealed that the main reasons for this include a higher risk awareness in the critical infrastructure sector in the role of provider, greater public pressure, as well as the regulatory framework and consequently an improved security consciousness.

Further research on the analysis of conformity and maturity in existing information security management systems has been conducted with regard to risk management as a central component in the management of information security. For this purpose, a defined number of companies were surveyed on their risk management practices. In addition to the methods or frameworks used, the procedures for identifying, assessing, and treating the identified risks were examined in detail. Furthermore, the documentation of the systems employed, and the top risks identified at the end served as the basis for data collection. Within the companies,

more than half had adopted a risk management approach based on a standard. Additionally, a distinction could be made between a standardized risk methodology and an asset-based methodology, with the difference lying in whether risks are considered for business processes or in the detailed assessment of risks to company assets. There were also differences in the investigations concerning qualitative or quantitative risk analyses, with the companies surveyed predominantly employing a qualitative strategy depending on their size and the systems and resources available. The following problems and challenges in risk management were identified in the companies surveyed. A central issue is the selection of the risk methodology or its adaptation to the requirements of the companies' business models. Another essential point is the lack of an approach for a structured procedure in risk identification.

Once risks are identified, the next step is to assess and evaluate their criticality. The research found that the surveyed companies often apply incorrect or inadequate approaches due to a lack of specific requirements within information security standards such as ISO 27001. Due to the absence of standardization, a structured procedure was established and proposed in the research. Since risk analysis, as identified in previous research findings, is a primary point of reference for deviations and non-conformities during audits, a focus on this area within the information security management system is necessary.

The *assessment of information security and process maturity within information security management systems in companies* showed that, after the successful analysis of non-conformities and risks within the business processes of information security management systems (ISMS), and to gain a holistic view of the overarching processes in conjunction with information security, further details of process maturity in ISMS. This involved an investigation into selected companies into audit results, how metrics and key figures are determined, and which are measured and used as indicators to achieve information security objectives. Criteria for collecting these key figures, such as frequency, standard utilization, system support, and deviations in audits related to missing monitoring through key figures, were identified. Key figures in management systems are fundamentally important because they enable the ongoing improvement process within the PDCA cycle to be measured and controlled.

Within the framework of information security management systems (ISMS), it is necessary to define objectives to achieve protection goals—confidentiality, availability, and integrity of information and data—and to monitor their achievement using key figures. A widely used key figure is the participation rate of employees in awareness training, an

indicator that is reviewed annually in the management review with the executive management. The investigation determined how many key figures are generally in use within the company and how frequently they are measured. Furthermore, it was found that the majority of management systems have defined manual collection of key figures. A significant problem was the appropriate selection of key figures that accurately reflect reality in the business process and ensure information security. The result of the study was that, in the absence of structured approaches and without the use of automatically determined key figures, reporting is only limited in its ability to provide a comprehensive overview of the overall state of information security. Additional approaches are needed, which are the subject of further research questions.

As part of further investigations into the topic, it has been shown which existing maturity level assessments within organizations exist. To do this, the ISO27001 structure was first analyzed in relation to a potential mapping. Based on standards for maturity assessment, such as the CMMI model with its six levels or other industry standards, a procedure model for maturity evaluation was identified and designed. As initially discussed, a regulation for weighting the individual areas of ISO/IEC 27001 had to be established, since findings in the audit chapters of the standard are assessed more critically than those in Annex A of the standard. The aim was to develop a calculation for an overall maturity level and to set a minimum value for it, from which it becomes apparent to organizations whether they have achieved a defined conformity with the requirements and could expect fewer findings in audits. Recommended measures for the use of such an assessment and its ongoing implementation within continuous improvement processes included regular reviews and self-assessments. Further modifications later in this research led to additional results and improved applicability within organizations.

Finally, with this doctoral thesis, could be underlined that information security topics pose significant challenges due to more and more inclusions of topics like sustainability issues, as the increasing complexity of systems requires more data and information to be securely managed. The existing gap lies in the insufficient overall overview of the current state of information security, combined with risks related to sustainability in the pursuit of corporate objectives. The *Improvement possibilities for measuring The Maturity Of Information Security Management Systems Considering Sustainability* are the result of this doctoral research.

For this reason, a mapping of the requirements from ISO 27001 for an Information Security Management System (ISMS) and sustainability requirements was developed as part of the implementation. The focus was on the measurability of fulfilling these requirements through achievable key figures and, in a further step, on assessing the process maturity within the requirements. The desired accuracy of measurement and the subjective assessment of whether requirements are fully or only partially met present a challenge. Due to the varying criticality of requirements within an ISMS concerning main chapter topics and issues in the technical, organizational, personal, and physical security areas of Annex A, different importance criteria were established, based on which maturity levels were subsequently calculated. As a fundamental concept for assessing maturity levels, the CMMI model was utilized here. This approach makes it possible to evaluate individual areas of the information security management system and to separately document the sustainability assessment and the level of information security. The new key figure ISSI comprehensively considers the relationship between information security and the sustainable implementation of requirements in the areas of environment, social issues, and governance. This ensures a holistic view from the perspective of top management in regular reporting periods, such as the annual management review of the ISMS. To test the applicability of the new approach and the usefulness of the new key figure, an exemplary application was carried out in a selected company that operates data centers in the IT services sector with sustainable waste heat utilization as one of its main business fields. After the assessment matrix was transmitted, the key figures were determined, and the maturity levels were evaluated.

The ISSI key figure calculated was discussed with management for the current reporting period. Additionally, the company examined the information security assessment using the defined criteria and key figures related to adaptation and adjustment to existing business processes. In a summarizing survey form, input was provided regarding improvements and the further development of the approach as feedback. Clear positive responses were achieved concerning the key figure and the approach, to obtain an indicator for a comprehensive view of information security, the status of compliance before audits and certifications, as well as the implementation of sustainability aspects as a business strategy and compliance requirement during reporting periods.

The hypothesis that a better overview of process metrics more precisely represents the risks associated with implementing requirements for sustainability and information security, thereby making a significant contribution to their avoidance or management, was proven

within the scope of the research work. Companies still have the opportunity, through a clear mapping of the requirements from information security and sustainability, to immediately adjust the measurement of the achievement of corporate goals and to eliminate gaps and associated risks. Based on previous research related to this work, it is known that collecting key figures and thus optimizing measurement and targeted achievement of goals can only be implemented if it also results in increased operational efficiency across all business areas. Without explicitly emphasizing it, it should be noted that preventing security incidents involving data leakage, loss, or compromise generally supports the maintenance of business operations and overall competitiveness.

In summary, extensive literature research enabled analysis of the technology's historical development and current state. This requires consideration of the additional requirements in the fields of information security and sustainability. Furthermore, specific instruments were examined as drivers for implementing sustainability, particularly the economic aspects of the circular economy, considering information technology and information protection. Insights were documented based on studies and surveys. Additionally, it was shown that relationships exist between risks and inadequate implementation within the continuous improvement process in surveyed and audited companies, highlighting the urgent need for a consistent overview of key figures and process maturity. Using these findings, existing maturity models and key figure systems in management systems were examined and evaluated. After mapping sustainability requirements to the requirements of the ISO/IEC 27001 information security standard, the need for a new key figure, the ISSI (Information Security and Sustainability Index), emerged, providing a unified perspective. It also became clear that a central scoring system using the ISSI metric could significantly support the achievement of these goals, based on the investigations of audited companies and detailed applications.

This doctoral thesis clearly demonstrated that companies need a holistic view of both current trends related to securing their information, data, and thus their business foundations, but this now must be done in combination with considering sustainability in order to remain competitive.

As a further step for future research based on this, the collection of data and key figures could also be automated, system-controlled, and visualized, based on feedback from the exemplary implementation. This would reduce manual effort and enable a real-time overview of changes in the overall maturity level and the ISSI key figure. As mentioned by the surveyed company,

this initial effort is mostly hindered by inconsistent measurement, a lack of figures, and, consequently, a lack of overview within the management system.

Another step involves considering financial aspects, such as cost savings resulting from the now-measured sustainability topics in operational and physical IT security. The expected reduction in security risks, as well as sustainability risks, could lead to an expansion of the model, which will be the subject of future research. This would also help to engage with emerging risks to data and information and the most valuable properties of companies, and to prepare for new trends in digitalization or digital transformation.