International Journal of Advanced Engineering and Management Research

Vol. 10, No. 01; 2025

ISSN: 2456-3676

A Comparative Study on Different Approaches Risk Management in Information Security Management Systems

Michael Matthias Naumann[1], Doru Alexandru Plesea[2], Marieta Olaru[3], Fabian Pitz[4]

[1]The Bucharest University of Economic Studies,
Piața Romană 6, Bucharest, 010374, Romania

[2]The Bucharest University of Economic Studies,
Piața Romană 6, Bucharest, 010374, Romania

[3]The Bucharest University of Economic Studies,
Piața Romană 6, Bucharest, 010374, Romania

[4]The Bucharest University of Economic Studies,
Piața Romană 6, Bucharest, 010374, Romania

doi.org/10.51505/ijaemr.2025.1007 URL: http://dx.doi.org/10.51505/ijaemr.2025.1007

Received: Jan 19, 2025 Accepted: Jan 29, 2025 Online Published: Feb 06, 2025

Abstract

When setting up and maintaining an information security management system, identifying risks and their treatment is a fundamental aspect. Due to the necessary alignment of the standards with the high-level structures of the ISO standards, individual standards such as ISO/IEC 27001 do not specify any specific requirements for a concrete risk analysis methodology. This leads to variations and adjustments in implementation within companies, resulting in non-conformities as well as inadequate implementation, which introduces further risks. Another challenge is the implementation of the risk methodology within integrated management systems with their different goals and approaches. The purpose of the paper is to highlight the challenges during risk management using different methods to identify, measure, and treat risks from an asset or process perspective. Furthermore, implementations of risk analyses at interviewed companies in practice will be considered to analyze and evaluate concrete problems in adapting risk analysis methodologies to the requirements within the companies. The results of the research show what other risks can arise if a methodological approach or treatment of risks is insufficient, as well as what can be an approach for a simplified structured and compliant approach of risks.

Keywords: risk management, information security risks, information security management systems risk analysis and assessment methodology.

Vol. 10, No. 01; 2025

ISSN: 2456-3676

1. Introduction

It is mandatory for companies of a defined size to implement risk management. For smaller companies, it is not mandatory, but it should be considered a management discipline to achieve company goals.

If a company commits itself to implementing a management system according to a standard whether due to market requirements or self-interest, then risk management is a fundamental part of the requirements.

When selecting a suitable risk management approach, the industry and thus the core processes, as well as existing implementations, play a decisive role in companies.

Another challenge with current management systems is the integration of different perspectives and requirements of the individual cross-sectional processes. For example, in the context of digitalization, a production company may not only need to provide proof of quality assurance through a quality management system (QMS) but also demonstrate appropriate assurance of information security via an information security management system (e.g., according to the international standard ISO/IEC 27001).

The implementation of requirements and measures in this regard requires an analysis of the business processes and corporate values within them. The subsequent risk analysis is crucial for identifying and treating risks within the business processes.

Due to the different approaches to topics such as quality, information security, but also environmental or energy management, there are no clear guidelines for the methodology of risk management. This leads to inconsistent implementation in companies with room for lack of risk assessments and inadequate implementation of treatment measures.

This paper is intended to present methodologies and current challenges regarding the risk analysis and as well as summarize a simplified approach.

1.1 Review of the scientific literature

The management of risks within management systems is considered in numerous scientific articles focusing on approaches and the associated challenges. There are both international and national standards that support the implementation through templates. In Efe (2023), selected risk management frameworks are analyzed and compared with regard to their approaches. Among other things, it was identified that the lack of knowledge and understanding of the risk management process as well as the need for monitoring and continuous improvement are significant challenges. Studies on the adaptation of common standards for risk assessment have been conducted, such as Johan et al. (2019), which explored the NIST 800-30 standard method.

Vol. 10, No. 01; 2025

ISSN: 2456-3676

One of the main reasons for the importance of the appropriate selection of risk management is that information security "covers areas such as physical and environmental security, organizational structure, human resources and the technologies used" (Barraza de la Paz et al., 2023).

Due to the application-specific requirements of risk management within companies or specialized organizational units, such as information technology, there is a need to define universally applicable technical and organizational models. This topic has been extensively examined in various studies, including(Aswat & Carolin, 2024), who stated that 'information technology plays a crucial role in risk management.

Within the selection of risk management methods for use in companies, both process considerations and system-side conditions determine the selection and thus the level of detail of the analysis of risks. To this end, "the advantages, and barriers in the approach of risk management in the industrial sector" were investigated in (Ispas et al., 2023). A common example of the different perspectives within an integrated management system is the combination of quality and information security, since in addition to the selection of the business processes to be assessed in quality management systems, different approaches to risk identification, consideration and treatment are pursued here than in information security.

As the integration of management systems increases, an overarching approach becomes more necessary. For instance, the 'FMEA suitability for assessing IT risks' was explored as part of an 'improved FMEA' (Subriadi & Najwa, 2020).

In the context of ISO/IEC 27001 and the IT sector, it has been demonstrated that 'risk assessment is one of the most time-consuming and crucial steps involved in developing an information security strategy for a company' and that 'it is imperative that each and every potential risk be identified. (Kitsios et al., 2023). The selection of suitable approaches depends on the level of detail required in the risk assessment, which may be conducted using qualitative or quantitative methods While (Melaku, 2023) states that "Qualitative assessment does not assign a dollar value to the assets; rather, it is mainly focused on the scenario-based assumption of the values of each asset" (Majka, 2024) examines the combination of qualitative and quantitative risk analysis using a semi-quantitative method to "illustrate how semiquantitative risk assessment (SQRA) can be effectively implemented in various sectors".

To address challenges and gaps from the perspective of compliance with standards, Naumann et al. (2024) examined the number of non-conformities in risk management during certification audits on information security at selected companies, identifying correlations and critical areas for improvement. This observation in specific industrial sectors was examined by (Lampe et al., 2024) for the relationship between risk analysis and current implementation of security requirements and the associated effects within "critical infrastructures" .

Vol. 10, No. 01; 2025

ISSN: 2456-3676

Further research from the perspective of IT service management according to ISO/IEC 20000-1, shows similar results and, due to the lack of detailed requirements, suggests an adapted approach to risk analysis according to the standards for information security, for example „the risk analysis required by the service management system can be completed with the one from the information security management system“ (Ionescu et al., 2020).

As an important point within the continuous improvement process of companies, appropriate models were developed and investigated to show the "alignment of cyber security measures with evolving threats and organizational changes“ (Tarakçı & Gönül, 2024)

Further developments in terms of digitalization, such as the use of AI, underline the crucial importance of risk management within companies. For example, "the interfaces between an information security management system (ISMS) and an AI management system (AIMS)" are examined, based on the requirements that "The EU AI Act (AIA) mandates the implementation of a risk management system (RMS) and a quality management system (QMS) for high-risk AI systems" in (Pötsch, 2024).

1.2 Research question and research objectives

The aim of this research paper is to examine the current state and the existing heterogeneity in the implementation of risk analysis for an information security management system (ISMS) and to highlight the different approaches, including the associated non-conformities with standard requirements such as the ISO/IEC 27001.

Additionally, this paper will explore which methodologies have been examined in scientific research, which standards for risk management exist and how selected and evaluated companies apply this knowledge in their risk analyses will also be considered in detail. Another objective is to analyze detailed challenges in interaction with other factors such as integration of several management systems or the lack of system support for risk calculation and treatment.

The hypothesis is that with a simplified, structured approach and an understanding of the effects of individual criteria, companies can implement an initial, appropriate risk analysis for information security ensuring conformity with the standard’s requirements.

2. Method

The authors analyze different common standards for risk management in information security, as well as general approaches to the calculation and treatment of risks. Furthermore, a qualitative approach was used to investigate recurring challenges in the implementation of risk analysis among a selection of surveyed companies. . For this purpose, 16 companies were examined along with their audit results within the certification of information security management systems (ISMS) according to ISO/IEC 27001 during the period 2022-2024

Vol. 10, No. 01; 2025

ISSN: 2456-3676

Table 1: Identified approaches of risk management in evaluated companies

Number of evaluated companies Period of evaluation	16 2022-2024
The percentage of companies with multiple management system	62,50%
The percentage of companies with a quantitative approach of risk analysis	6%
Most adopted risk management framework in the companies	BSI-Standard 200-3
Frequent identified risks	lack of resources, data leakage, risk management system non-availability

Source: Authors' own research.

It was examined which procedures were used within the companies regarding risk analysis for the management system. These include:

- List of possible risk management standards for information security
- List of methods for qualitative vs. quantitative risk analysis
- Use of an integrated management system or several management systems
- Performing the risk analysis with tool support or Excel
- Risk score calculation, metrics
- Top Risks, Number of Risks,
- Non-Conformities regarding the Requirements for risk management during Certification Audits
-

Based on the results, we conclude by looking at which approaches are most suitable for deployment and which remaining challenges remain.

3. Results

The main problem with risk analysis begins with the selection of a suitable risk management method for the processes, information or assets that need to be protected.

3.1 Results of the evaluation of risk management frameworks used by analyzed companies

The methodology for risk analysis used by the evaluated companies was based on the following frameworks (Table 2).

Vol. 10, No. 01; 2025

ISSN: 2456-3676

Table 2: Risk management frameworks used by evaluated companies

Risk management frameworks	Percentage of evaluated companies (%)
BSI-Standard 200-3	31
ISACA IT Risk Framework	6
ISO/IEC 27005	19
FMEA based	13
No standard / mixed	31

Source: Authors' own research.

Due to the intended compatibility with all management systems, there is no defined risk management standard specifically for information security or the ISO/IEC 27001 normative standard requirements.

This results in heterogeneous implementations by companies seeking certification leading to a lack of or insufficient implementation of risk assessments and treatments.

In the following, the risk management standards used by the analyzed companies will be considered.

a) The standard; ISO 31000:2009 is the high-level standard for risk management making it universally applicable. It is considered here to describe the underlying approaches of the other, more specific standards.

"Risk management involves coordinated activities to steer and manage an organization in relation to risks" (International Standards Organization (ISO), 2023)

Within ISO 31000, there are no specific requirements for the exact calculation and identification of risks. Here, a high-level process is described that consists of the following phases (ISO, 2023):

- Establishing the context
- Communication and consultation
- Risk assessment with sub phases: risk identification, risk analysis, risk evaluation, risk treatment
- Monitoring and review

From the perspective of information security, this defines only a general, process-based approach to risk analysis.

b) Failure Mode and Effects Analysis

FMEA is a method of avoiding known errors within processes. The risk calculation is based on significance, occurrence, and findability/detection.

Vol. 10, No. 01; 2025

ISSN: 2456-3676

The calculation of the so-called risk percentage (RPZ) is carried out using the following formalities:

RPZ = Significance (B) x Occurrence (A) x Probability of Detection (E) (1) .
Since many companies already have a quality management system in place before introducing information security management systems, a risk methodology based on an FMEA approach often already exists, such as the use of criteria for the detectability of risks. This then leads to a combination of quality and information security.

A disadvantage from an information security perspective is that the FMEA does not investigate the effects of damage caused by threats but only examines defective components or products. The FMEA therefore only analyses external misconduct and its probabilities.

c) The ISO/IEC 27005 standard is not a normative standard like ISO/IEC 27001, which can be used as a basis for certifications. This means that ISO/IEC 27005 "supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach" (ISO, 2022).

In contrast to the high-level view of ISO 310000, the impact of risks is considered more than just consequences in the context of information security.

Furthermore, different from goals such as ensuring the quality of products or services, the 3 main principles of information security are the preservation of confidentiality, availability, and integrity of information,

For this reason, the consideration of risks within ISO/IEC 27005 is more focused on damage or loss.

In detail, ISO/IEC 27005 speaks during the risk identification of a „degree of damage or costs to the organization caused by an information security event“ (International Standards Organization (ISO), 2022).

In addition, the model shows that only threats that encounter a vulnerability pose a risk to an asset. A threat without a vulnerability does not pose a risk.

d) According to the BSI-200-3 standard

Risk Analysis based on IT-Grundschutz (BSI, 2018), the entire risk analysis process is a fundamental component of information security management. The identification of individual risks is carried out by assessing the frequency of the occurrence of the risks and the amount of damage caused by the risks in the event of an incident . Various safety measures are taken to treat the risks, the effectiveness of which can be tested by comparative analyses.

Vol. 10, No. 01; 2025

ISSN: 2456-3676

A risk analysis is required for all target objects that have a high or very high need for protection in at least one of the three basic values of confidentiality, integrity or availability, or - cannot be adequately mapped (modelled) with the existing building blocks of IT baseline protection, or - are operated in application scenarios (environment, application) that are not provided for in the context of IT baseline protection

- Creation of an overview of possible hazards
- Extension of the overview with additional hazards
- Risk assessment / classification of risks
- Treatment and monitoring of risks
- Consolidation with the security concept

When assessing the risks, only a mapping to the 4 risk categories with Low, Medium, High, Very High is carried out here (Figure 1).

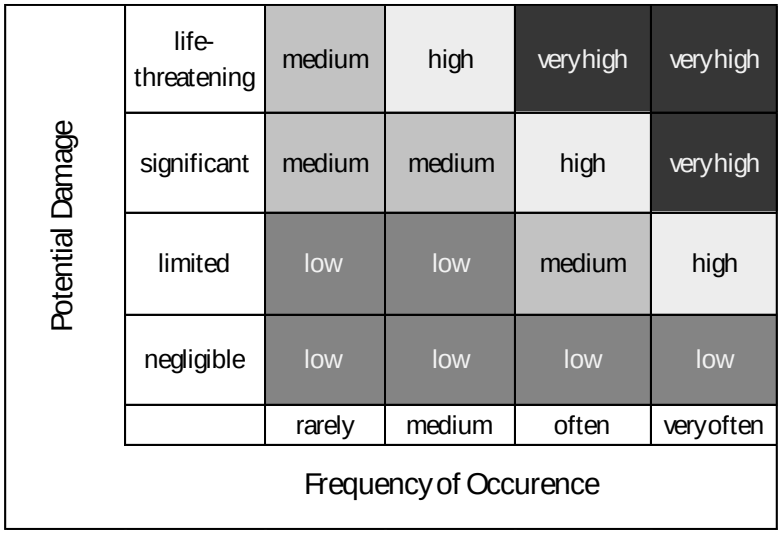

Figure 1: BSI risk matrix, Source: BSI Standard-200-3,

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2003_en_pdf.html?nn=908032

The BSI's threat catalogue, which is used by most of the companies surveyed to define threats to company assets or processes, serves as a helpful template.

Threats are all events that could jeopardize security and harm the company by exploiting a vulnerability. Examples include:
Natural disasters, system failures, accidental human intervention, malicious behavior, theft, and so on.

Vol. 10, No. 01; 2025

ISSN: 2456-3676

The Risk IT Framework. The Information Systems Audit and Control Association (ISACA) defines a risk equation as part of The Risk IT Framework (ISACA, 2020):

Risk = Threat Frequency x Vulnerability x Asset Value (2)

Threat frequency: How often is a particular threat expected within a given time frame, such as based on an estimate from previous incidents or threat news.
Vulnerability: The likelihood that a vulnerability will be exploited, based on existing security controls.

Asset value: The importance or value of the assets that could be affected by the threat. This can include tangible assets such as hardware and intangible assets such as data and reputation.
The procedure for calculating risk using the ISACA risk equation is:

- Identifying the asset
- Financial valuation of asset value
- Identifying the threats that could cause damage or loss
- Assessing threat frequency
- Assessing vulnerabilities and how vulnerable each asset is to the identified threats.
- Calculating risk by multiplying the frequency of the threat by the vulnerability and value of the asset.

The use of this risk management framework allows a quantitative view of risks.

3.2 Results of the analysis of asset-based risk management vs. scenario-based risk management

There are two main types of information security risk assessments: asset-based and scenario-based.
Asset-based risk assessment focuses on identifying and assessing the risks to specific information assets, such as customer data, financial data, and intellectual property.

Both approaches to risk assessments include the following steps:
- Identify the assets/information assets or business processes that need to be protected
- Identify the threats and vulnerabilities that could affect any information asset or business process.
- Assess the likelihood and impact of each threat and vulnerability.
- Prioritize risks based on their likelihood and impact.
- Develop and implement risk mitigation strategies to reduce risk to any asset or business process.

Scenario-based risk assessment focuses on identifying and assessing the risks to specific business processes and allows for a more holistic view of the organization's information security risks.

Vol. 10, No. 01; 2025

ISSN: 2456-3676

In the case of integrated management systems and quality management systems, a process analysis is generally carried out. In the case of information security management systems, the asset-based approach predominates, but there is a risk of a purely technological perspective from an IT viewpoint for hardware, software, mobile devices and thus the failure to consider other risks involved for business processes, such as financial risks or physical security.

3.3 Results of the analysis of quantitative vs. qualitative risk analysis

There are several options for conceptual approaches to risk analyses within management systems in the field of information security. Companies have the option of conducting a quantitative or qualitative risk analysis. In practice, when implementing management systems, companies do not have any support in correctly recording assets and then quantifying the impact ideally supported by a system. For this reason, the use of qualitative risk analysis is much easier to implement.

Risk measurement in risk analysis can be qualitative, quantitative, or a mixture of both:

- *Qualitative Risk Analysis:* Includes descriptive terms to identify the severity and likelihood of risks. Often, categories such as High, Medium, and Low are used to evaluate both impact and likelihood.
- *Quantitative Risk Analysis*: Includes numerical and statistical techniques for measuring risk, such as expected monetary value (EMC), Monte Carlo simulations, and sensitivity analysis. It quantifies probability and impact in numerical terms and provides a more detailed risk assessment.

Of the companies surveyed, 69% use an Excel-based solution. 13% use a document management system or ticketing system, and another 13% have a tool to perform risk analysis (Table 3).

Table 3: System support for risk analysis used by evaluated companies

System support for risk analysis	Percentage of evaluated companies (%)
Excel	69%
SharePoint / JIRA	13%
Risk Management / ISMS Tool	19%

Source: Authors' own research.

The tool support then also allows a quantitative risk analysis, which, however, is only carried out by one of the companies surveyed.

In only a few industries quantitative risk analysis is established for management systems. The excessive effort involved in quantifying the effects of damage, as well as the lack of system support play a role here (Table 4).

Vol. 10, No. 01; 2025

ISSN: 2456-3676

Table 4: Risk analysis approach used by evaluated companies

Risk analysis approach	Percentage of evaluated companies (%)
Qualitative risk analysis	6%
Quantitative risk analysis	94%

Source: Authors' own research.

3.4 Evaluation of the challenges with risk management approaches inside analyzed companies

A big problem in fulfilling the requirements for risk management and being compliant with the certification standards is the selection of the appropriately sized risk methodology.

The main problems identified by the companies examined were as follows:

a) Risk methodology

- Mixture of different risk methodologies (FMEA, ISO27005, ...)
  Several different risk analyses based on organizational conditions, such as geographical distribution of the company and requirements only for certain parts of the company without group-wide definition
- Problems in the ongoing consideration of existing and new risks within the annual consideration. The target risk values achieved were not carried over to the new observation period.

b) Risk identification

- Definition of risks with an estimate without a holistic view. No structural approach to the identification of risks, e.g., by means of a protection needs analysis or the use of standard hazard catalogues.
- focusing on IT risks, no consideration of other supporting processes
- Insufficient grouping of similar company assets with the same risks and thus generating too many risks
- No additional system tests, controls or checks to find further vulnerabilities

c) Risk assessment

- No correct definition of risks in detail for **Inherent Risk**: This will be the risk without existing controls, **Residual Risk** This will be the risk with existing controls, **Expected Risk**: This will be the risk what is expected after implementing the risk treatment measures.
  This means that companies are starting the risk determination sometimes seeing the risk treatment only with existing measures instead of defining additional risk measures to bring the risk to a defined target level
- Inadequate approach of risk calculation such as multiplication vs. addition
  For the companies surveyed only 1 company has a risk calculation based on adding the values of e.g. impact and probability. This results in a small range of values so that it can happen that risks will not be determined correctly.

Vol. 10, No. 01; 2025

ISSN: 2456-3676

- Non-existent or insufficiently defined criteria in risk assessment, so that the determination or calculation of the risks is not reliably reproducible.
  For the companies analyzed, a very high variation of the ranges in the criteria was evaluated.

Table 5: Risk matrix model used for risk assessment by evaluated companies

Risk matrix model used by evaluated companies	Percentage of evaluated companies (%)
5x5 risk matrix	25%
4x4 risk matrix	19%
3x3 risk matrix	19%
5x5x10 risk matrix	6%
3x3x3 risk matrix	6%
5x3 risk matrix	19%
4x4x4 risk matrix	6%

Source: Authors' own research.

This results in a low number of values for criteria (3x3), leading to a much less precise risk determination compared to risk matrices with larger ranges (5x5) (Table 5).

- Numeric vs. categorized determination and visualization of risks in different ways were evaluated for the companies surveyed. The risk categories can be ranked with categories like low, medium, high, critical, or they can be calculated. The representation can also vary (Figure 2). This results in a different recognition of risks.
-

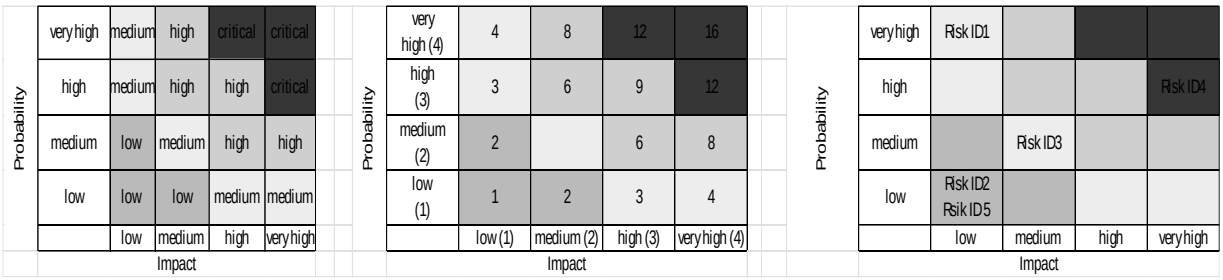

Figure 2: Examples of risk matrix visualizations used by evaluated companies
Source: Authors' own research.

- The calculation was also done with numerous factors. There are two-dimensional or multi-dimensional calculations. The use of more than 2 factors for risk calculation can also result in different presentations. Additional criteria like detectability, besides the Impact and Probability will result in a more complex determination.

d) Risk treatment

Vol. 10, No. 01; 2025

ISSN: 2456-3676

- Tracking risk treatment measures: One of the most recent issues during audits of risk management requirements inside management systems is the missing or overdue tracking of the risk measures.
- No defined risk acceptance criteria: A limit must be set as to the level of risk up to which risks may be accepted. Any risks above this limit should be addressed

4. Discussion

Due to the lack of specifications and variability in the evaluation of management systems, a simplified but structured approach for risk analysis in information security management systems should be defined.

A *simplified approach for risk analysis and assessment methodology proposed by authors*

The following steps are a simple sequence:

- Grouping the discovered assets based on predefined ISO/IEC 27005 groupings by their owner
- Identification of the associated threats
- Considering assets with high protection needs and risks with high criticality
- Try to involve knowledge carriers and derive scenarios
- Setting a simple risk probability in 3-4 levels, e.g., often, frequently, rarely, very rarely
- Determining of the amount of damage according to ISO 27005 Risk Management in 3-4 levels (low, significant, critical, and catastrophic)
- Calculating risk values and defining a maximum of 4 risk categories with a traffic light color scheme, whereby risk acceptance must be defined for lower threshold values.
- Fixed by simplified risk treatment options such as treat or accept
- Annual transfer of the adjusted risk values to a new risk analysis

The topic of information security risk management is not sufficiently regulated in the management review in such a way that different and inadequate approaches and methodologies are used. The risks that are not addressed in this way lead to further risks or to the impairment of business processes.

The purpose of the paper was to show that risk analysis as part of the planning phase of the PDCA cycle must be considered much more than is currently implemented by many companies.
Within audits to check conformity, but also regarding security incidents, a suitable definition and selection of risk analysis plays a decisive role in the protection of corporate assets.
As the evaluation of the results of the companies surveyed about risk analysis showed, the current problems arise from the non-existent requirements for risk management.
Even minimal changes in the calculation of the risk value or in the differentiation of criteria lead to different interpretations, strategies and measures as result of the risk analysis. Here, a normative and thus standardized approach would be to implement organizational and technical specifications in a targeted manner and thus reduce information security risks.
This paper defines a approach that can be applied at any time in an integrated management system at a high-level level.

Vol. 10, No. 01; 2025

ISSN: 2456-3676

In the area of the ISO/IEC 27001 standard, it would be easy to implement the existing requirements of ISO/IEC 27005 standard and thus achieve comparable and conceptually consolidated results.
Since the number of companies surveyed is not generally meaningful, a broader survey would be necessary to obtain further details.

Another very important topics shown in this paper are the conflicts in the integration of different management systems such as for quality, information security and other topics using the example of risk analysis. The problems of improved visibility of risk management and adjustments with the continual improvement process should be considered with further research so that the visibility of costs and threats within the company's processes is improved.

References

Aswat, I., & Carolin, A. (2024). The Role of Information Technology in Risk Management in the Service Sector (Case Study on Accounting Service Firms in Pontianak) (S. 65–73). https://doi.org/10.2478/9788367405850-007

Barraza de la Paz, J. V., Rodríguez-Picón, L. A., Morales-Rocha, V., & Torres-Argüelles, S. V. (2023). A Systematic Review of Risk Management Methodologies for Complex Organizations in Industry 4.0 and 5.0. Systems, 11(5), Article 5. https://doi.org/10.3390/systems11050218

BSI. (2018). BSI-Standard 200-3: Risk Analysis based on IT-Grundschutz. BSI. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2003_en_pdf.html?nn=908032

International Standards Organization (ISO). (2022). ISO/IEC 27005:2022—Information security, cybersecurity and privacy protection—Guidance on managing information security risks. ISO.org. https://www.iso.org/standard/80585.html

International Standards Organization (ISO). (2023). ISO 31000:2018 Risk management—Guidelines. ISO.org. https://www.iso.org/standard/65694.html

Ionescu, R. C., Olaru, M., Lampe, G. S., & Fogoros, T. E. (2020). A STUDY ON INFORMATION SECURITY IMPACT ON THE DELIVERY OF IT MANAGED SERVICES. Vol. 01, 958–965. https://www.researchgate.net/profile/Bassel-Diab/publication/342124082_BASIQ_2020_Conference_proceedings/links/5ee37056458515814a583fe1/BASIQ-2020-Conference-proceedings.pdf.

ISACA. (2020). ISACA's Risk IT Framework Offers a Structured Methodology for Enterprises to Manage Information and Technology Risk. ISACA. https://www.isaca.org/about-us/newsroom/press-releases/2020/isacas-risk-it-framework-offers-a-structured-methodology

Ispas, L., Mironeasa, C., & Silvestri, A. (2023). Risk-Based Approach in the Implementation of Integrated Management Systems: A Systematic Literature Review. Sustainability, 15(13), Article 13. https://doi.org/10.3390/su151310251

Vol. 10, No. 01; 2025

ISSN: 2456-3676

Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2023). The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector. Sustainability, 15(7), Article 7. https://doi.org/10.3390/su15075828

Lampe, G. S., Massner, S., Naumann, M. M., Pitz, F., Olaru, S.-M., & Wittstock-Lampe, A. (2024). A Quantitative Analysis of Information Security Management System Audit Results in Critical and Non-Critical Information Technology Infrastructure. International Journal of Advanced Engineering and Management Research, 09(03), 01–17. https://doi.org/10.51505/ijaemr.2024.9301

Majka, M. (2024). Semi-Quantitative Risk Assessment: Bridging the Gap Between Qualitative and Quantitative Methods.

Melaku, H. M. (2023). Context-Based and Adaptive Cybersecurity Risk Management Framework. Risks, 11(6), Article 6. https://doi.org/10.3390/risks11060101

Pötsch, J. (2024). Interplay of ISMS and AIMS in context of the EU AI Act (arXiv:2412.18670). arXiv. https://doi.org/10.48550/arXiv.2412.18670

Subriadi, A. P., & Najwa, N. F. (2020). The consistency analysis of failure mode and effect analysis (FMEA) in information technology risk assessment. Heliyon, 6(1). https://doi.org/10.1016/j.heliyon.2020.e03161

Tarakçı, E., & Gönül, A. M. (2024). Risk Analysis and Assessment Framework for Cyber Security in Management Systems. OHS ACADEMY, 6(3), Article 3. https://doi.org/10.38213/ohsacademy.1402624