International Journal of Advanced Engineering and Management Research

Vol. 9, No. 03; 2024

ISSN: 2456-3676

A Quantitative Analysis of Information Security Management System Audit Results in Critical and Non-Critical Information Technology Infrastructure

LAMPE Georg Sven[1], MASSNER Stephan[2], NAUMANN Michael Matthias[3], PITZ Fabian[4], OLARU Stelian-Mircea[5] WITTSTOCK-LAMPE Anke[6]

[1,] The Bucharest University of Economic Studies, 010374, Romania
[2,] The Bucharest University of Economic Studies, 010374, Romania
[3,] The Bucharest University of Economic Studies, 010374, Romania
[4,] The Bucharest University of Economic Studies, 010374, Romania
[5,] The Bucharest University of Economic Studies, 010374, Romania
[6,] The Bucharest University of Economic Studies, 010374, Romania

doi.org/10.51505/ijaemr.2024.9301 URL: http://dx.doi.org/10.51505/ijaemr.2024.9301

Received: Apr 08, 2024 Accepted: Apr 17, 2024 Online Published: May 02, 2024

Abstract

Due to the increasing frequency and severity of Information Security (IS) and Cyber Security (CS) incidents, organizations are focusing on the secure design of technical Information and Communication Technology (ICT) systems as well as organizational development and process orientation within the critical and non-critical Infrastructures. This procedure serves the purpose of reliably providing the official and corporate services that are essential for maintaining social and economic activities. By fulfilling the legal requirements, critical service organization should also be able to avert potential cross-sector and cross-border disruptions as well as deal with serious security incidents. In addition, the operators of critical services are required to certify the scope of the established management system in accordance with the recognized international standard for compliance with information security. This research focuses on the development of measurement models for management systems, which are based on the results of external audits and audit findings as part of an empirical analysis within critical and non-critical infrastructures. The audit findings regarding personnel knowledge gaps and organizational, technical and physical problems identified in the implementation and use of management systems in the consulting environment and in the audit of management systems are discussed in more detail.

Keywords: Information Management System Audit, Information Security International Standards, Critical and Non-Critical IT Infrastructure, Measurement Model Results.

Vol. 9, No. 03; 2024

ISSN: 2456-3676

1. Introduction

Efficient and reliable Business Processes (BP) regarding the information to be protected (Information Objects – IO) and their Information and Communication Technology (ICT)-supported systems/services (Supporting Assets – SA) to overcome complex operational company challenges are essential. This also includes certification in the line with the internationally recognized standard of information security Management Systems in accordance with ISO/IEC 27001 in all industries with Critical and Non-Critical Infrastructure.

Directive (EU) 2022/2557 of the European Parliament and of the Council focuses on resilience within the European Union (EU), regulating the various aspects in its member states such as compliance with standards and requiring their implementation into national law. Management systems certification is a formal process by which an authorized body, following an assessment, confirms that an organization's process, product or system meets certain predefined standards and requirements. These procedures include audits, analyses and ongoing monitoring of the certified scope and are carried out by accredited certification bodies and/or auditing companies or contractually appointed auditors. As a neutral, independent, impartial and integrity (N3I) auditor, this external service is provided professionally. By carrying out the external audit according to a predefined standard, the existence and productive operation of a MS or an Integrated MS (IMS) is officially confirmed. The external audit is an important mechanism for ensuring the effectiveness and continuity of MS by providing an independent assessment and confirmation of their proper operation. The importance of internal control factors in maintaining the accountability of auditors should be emphasized, especially during inspection emphasized (Febriana et. al., 2017, pp. 166-175). Here, the role of auditors in fraud detection and prevention in banks as well as to note the importance of risk assessment and system audits in improving fraud control (Olatunji et. al., 2017, pp. 290-306).

A critical infrastructure certification process verifies compliance with certain established standards and guidelines to ensure the security, robustness and resilience of infrastructure facilities that are critical to the functioning of a society. These inspections can be carried out internally or by external auditors and also support the continuous improvement of the security architecture. Therefore, operators of critical infrastructures wear a special responsibility for national security and the maintenance of public order and welfare. During examining characteristics of independent commissioners and audit committees on earnings management, it was found that reducing opportunistic earnings management has a significant effect (Mardjono et. al. 2020, pp. 569-587). In addition, the symbolic interaction of internal auditors in consultation activities was highlighted and the importance of mindset and social factors in improving communication within the Inspectorate General was emphasized (Nugraheni et. al., (2021, pp. 1-6). Several authors have found that performance audits contribute to accountability and performance improvements in audited public sectors (Morin, 2001, p. 99; Manaf, 2010, p. 2), while other studies found out, that performance audit had contributed little to accountability and performance improvements in the audited public sectors (Morin-Danielle, 2003, pp. 19-30;

Vol. 9, No. 03; 2024

ISSN: 2456-3676

Morins, 2004, p. 143; Reichborn-Kjennerud and Johnsen, 2011, p. 218; Reichborns, 2013, p. 681; Reichborn-Kjennerud, 2015, p. 18).

Critical Infrastructures (CRITIS) are ICT-supported systems, facilities, services and sub-areas that are essential for the functioning of a society and economy. These include, for example, basic water and electricity supplies, telecommunications, transport and traffic, medical care and government and financial services. Companies that provide critical services for more than 500,000 people through their corporate system infrastructure, for example in Germany, are required to register with the Federal Office for Information Security (IS) as operators of critical infrastructure. In cases where a corporate system infrastructure supplies services to no more than 500,000 people, it is classified as an operator of Non-critical Infrastructure (Non-CRITIS) according to the defined threshold values. The obligations as a CRITIS operator begin with identification of critical infrastructure and the Scope of Applicability (SoA), followed by reporting obligations, the implementation of cyber security and regular audits as proof. Bernard (2007, pp. 26-30) discusses the significance of Information Lifecycle Security Risk Assessment in extending information security programs to cover all forms of critical data. Olaoye et. al. (2019, pp.17-22) focused on performance audit and public sector budgetary efficiency, highlighting the significance of total quality management, public sector value, and government accountability system in enhancing efficiency. In recent years, there has been an increasing concern about cyber-attacks on monitoring and control devices responsible for supervising critical processes in critical infrastructures (Coppolino et. al., 2011, p. 5).

Furthermore, comprehensive measures for IT security must be implemented and maintained to ensure IS and Cyber Security (CS). This includes the development and continual updating of security concepts and strategies. In addition, regular inspections and audits are required to provide the relevant authorities with proof of compliance with regulations and the status of security measures. Gao et. al. (2011, pp. 109-116) emphasize the importance of quality data collection for developing robust performance models in infrastructure management systems. Ani et. al. (2019, pp. 1-16) examines approaches to protecting critical infrastructure that focus on modeling and simulating security risks. Foglietta et. al. (2020, pp. 1-16) propose the MHR (Mixed Holistic Reductionist) approach for modelling infrastructures, emphasizing the consideration of three different layers in each infrastructure. A failure or impairment of these critical infrastructures would have serious consequences for the economic stability of companies and administrative functions.

The consequences of a failure or impairment of Non-Critical Infrastructure are detrimental, but do not have any immediately serious effects on social coexistence, the economy or government functions. These include, for example, services and facilities that are more focused on comfort and entertainment. The analysis of important features of critical infrastructure has been proposed an integrated cyber security risk management framework to assess and manage risks proactively (Kure et. al., 2018, p. 6). Culot et. al. (2021, pp. 1-30) presented a comprehensive literature review and research agenda for the ISO/IEC 27001 standard. After 15 years of research, the authors outlined research opportunities to inspire interdisciplinary studies at the intersection of

Vol. 9, No. 03; 2024

ISSN: 2456-3676

information security and quality management. Critical infrastructures are closely interconnected with non-critical structures, which leads to mutual dependencies. Direct interruptions to company processes in energy supply and transport services can have far-reaching economic consequences, such as production downtimes with financial losses. Individual disruptions in critical areas can also lead to cascading effects that affect non-critical systems, such as a cyber attack on banking that could disrupt payments and related industries. Explicit security gaps in ICT-based systems in non-critical areas can become a threat through the exploitation of a cyber-attack and spread to critical infrastructure. Ultimately, efficient Communication, Coordination and Cooperation (3C) between critical and non-critical sectors is crucial for resilience and adequate response to disruptions or threats (Lampe et. al., 2022, pp. 911-919).

Today's Management Systems (MS) in Critical and Non-critical Infrastructures must evolve rapidly, as does the pace of innovative change in ICT-enabled business processes due to the increased incidence of cybersecurity risks (World Economic Forum, 2024, p. 7-8). Against this background, the established MS for IS in CRITIS and Non-CRITIS require a holistic view to assess the resilience and ability to deal with disruptions or personnel knowledge gaps and organizational, technical and physical problems. This involves a thorough examination of the MS in its entirety and in all its aspects at the respective company's locations. The audit is conducted according to predetermined guidelines regarding the duration and scope of the audit, which typically follow a three-year certification cycle. Surveillance audits are carried out in between these cycles, which are reduced in time scope but specifically defined according to the audit topics of requirements. During the audit, auditors determine compliance and deviations concerning the existing management system. Distinctions are made between major and minor deviations. Significant deviations can lead to a failed external audit, while minor deviations must be rectified by the next audit in order to meet the audited standard. The audit findings in Critical and Non-critical infrastructures that were identified during the implementation and use of Management Systems in the consulting environment and in the audit of MS are appropriate and suitable for this purpose. In this context, the included study focuses on identifying which aspects of the international ISO standard according to ISO/IEC 27001 lead to the most Non-Conformities (NC) in management systems during audits (internal/external) in Critical and Non-critical areas. Additionally, it is necessary to determine the success factors for MS certifications and the causes of Non-Conformities from various perspectives. Here, is a focus placed on aspects of continuous improvement and the evaluation of management performance as well as the establishment of Risk Management (RM). The listed aspects are analyzed based on the results of external audits conducted in various organizations in non-critical and critical sectors from 2019 to early 2024.

This analysis pertains to both the implementation practices and the effectiveness or maturity level of the respective aspects within the established information security management. Overall, the methodology to be used forms the aim-oriented identification and treatment of risks and opportunities for Information Security Management Systems (ISMS) in the NON-CRITIS and CRITIS areas. This provides companies with the opportunity to perform a focused compliance analysis when implementing and using MS in the consulting environment and to provide

Vol. 9, No. 03; 2024

ISSN: 2456-3676

appropriate treatment prior to management systems audits. This consideration as chance can be helpful in establishing a resilient and future-oriented organization.

2. Method

2.1 Purpose and objectives of the research

This study is based on an empirical analysis derived from the results of external audits which carry out by the N3I auditor and the resultant audit findings. The database is comprised of information and audit reports collected during external audits, as well as from publicly available management reports of 178 organizations. All information was thoroughly analyzed and the necessary data for the study was extracted. This approach allows for a detailed examination of the effectiveness and implementation practices of Information Security Management System (ISMS) within the organizations under review.

International standards such as ISO/IEC 27001 and ISO/IEC 27019 were used in the audits, sometimes combined with ISO 9001 as the auditing IMS. The combined audits were carried out by an audit team in which the author was involved. The audit findings included interviews with various employees during the audits.

The methodological analysis of audit deviations focuses on both critical and non-critical infrastructures, which are organizations and facilities of essential importance to the state and the community. The investigation centers on the extent to which audit results affect the maintenance and assurance of operational capability of these essential facilities. Specifically, it analyzes the particular deviations from the normative requirements that were identified and the potential risks they pose to supply security and public order. Furthermore, measures and strategic ISMS objectives are audited to check for compliance and identify findings to address them, thereby minimizing observation, irregularity, or even susceptibility to failures or impairments. The compliance analysis allows for an assessment of the current security and risk management of critical and non-critical infrastructure and provides starting points for their continuous improvement and prevention of severe consequences in the event of potential future disruptions.

The non-conformities as audit results were empirically tested using the calculation of the standard deviation, variance value, and mean value. The standard deviation (s) is calculated as follows:

$$s = \sqrt{\frac{1}{N-1}\sum_{i=1}^{N}(x_i - \overline{x})^2}, \tag{1}$$

x_i equals one sample value

$\bar{x}$ equals the mean of the sample and N equals the sample size

Vol. 9, No. 03; 2024

ISSN: 2456-3676

The subsequent hypotheses were tested:

1. There are more non-conformities in areas within the higher-level structural chapters (HLS) than in Annex A.
2. There are more non-conformities in Non-Critical Infrastructure operators than in Critical Infrastructure operators.
3. Overall, there are more nonconformities in areas within Annex A than in the higher-level structural chapters.

This is necessary to illustrate any correlations between audit deviations and threshold values of companies that provide essential services and exceed certain quantitative limits.

2.2 Data collection

This research focuses on the development of measurement models for management systems based on empirical analysis results from external audits and examination findings within Critical Infrastructure and Non-Critical Infrastructure areas. Therefore, procedural approaches and established practices essential for merging different management approaches and methods were audited.

Furthermore, various analysis techniques are applied, such as functional and dysfunctional methods for determining the criticality level and risk categorization of examination findings of established business processes. The minimum requirements for all sector-oriented companies within Critical Infrastructure and Non-Critical Infrastructure are based on the

- Main part according to ISO/IEC 27001 and the associated ANNEX A (included 114 Controls).

For CRITIS operators that are obligated to certification, additionally, the

- Main part according to ISO/IEC 27019:2020 must be complied with. The ISO-based requirements mostly refer to the requirements according to ISO/IEC 27001. The specific requirements set out in the various sections according to ISO/IEC 27019:2020 are aligned with an ISMS according to ISO/IEC 27001.
- IT-Security Catalogue 1a and 1b must be followed. Electricity and gas network operators are required to implement IT security technical minimum standards. The core requirement is the establishment of an ISMS in accordance with ISO/IEC 27001.
- Requirements catalogue according to BSI for the deployment of attack detection systems, with MUST, SHOULD, and CAN requirements, which are inclined towards an ISMS according to ISO/IEC 27001.

All specific requirements indirectly contribute to information and cyber security for CRITIS operators and are assigned to the security categories for appropriate and suitable comparability. The audited organizations, as operators of critical and non-critical infrastructure, are active in various industries, as shown in Table 1.

Vol. 9, No. 03; 2024

ISSN: 2456-3676

Table 1. List of operators for Critical Infrastructure (CRITIS) and Non-Critical Infrastructure (Non-CRITIS) in different sectors with ISMS regarding ISO/IEC 27001

Sectors	Organization	Operators of critical infrastructure	Operators of non-critical infrastructure
Energy	23	12	11
Information technology and telecommunication	25	13	12
Transport and Traffic	27	15	12
Health	24	10	14
Media and Culture	26	8	18
Water	25	15	10
Finance and Insurance	28	18	10
7 sectors	178	91	87

Source: Authors own elaboration based on audits regarding ISO/IEC 27001.

The organizations vary in their personnel size from Small and Medium-sized Enterprises (SME) with 5 employees in the scope of applicability to large organizations with over 1,500 employees. The results included input from 178 companies, located throughout Europe, with an annual turnover ranging from at least 2 million EUR to 2 billion EUR. Due to the ISO-based requirements to be audited, it was ensured that the focus of the questions was on compliance with information and cybersecurity. The interviewees, who are active at the strategic and operational level, were therefore guided through a standardized and predefined requirements protocol. Furthermore, the compliance analysis examines how companies integrate the requirements according to ISO/IEC 27001:2017 as an Information Security Management System (ISMS) and what the consequences of the audit findings can be in terms of threshold values, for instance concerning the necessity of introducing additional security and protection measures.

Special attention was given to the examination of findings on personnel knowledge gaps, organizational, technical and physical issues identified during the implementation and use of management systems in the consulting environment as well as in the auditing of management systems. The evaluation of the audit findings upon which this study is based includes only companies in the mentioned sectors from the CRITIS and Non-CRITIS areas. For data collection, anonym zed results and data from the audited companies regarding information and cyber security over the last 5 years were used.

3. Results and discussion

3.1 Criteria and interdependencies for external audits of Management Systems

Before audits can be carried out by auditing companies, they must first be officially approved by the respective accreditation body. Once this official approval has been granted, the appointed

Vol. 9, No. 03; 2024

ISSN: 2456-3676

auditors from certification companies can then assess the management system of other companies for conformity in accordance with the specified external certification procedures. The holistic assessment of the management system for the area of application (Scope of Applicability – SoA) at the respective locations (headquarters, other locations) is a central task. The auditing is based on specified standards with regard to the time required and the scope of the investigation and is usually based on a three-year certification cycle. Within the three-year certification cycle, specific monitoring audits are carried out in the second and third years, which are reduced in time to the requirements topics to be audited but are specifically defined.

An external N3I-acting auditor can, through an external audit on behalf of certification bodies, third-party auditing company, officially confirm the existence and effective implementation of a MS or IMS. The criteria and requirements that auditors from these auditing firms must adhere to when conducting such audits are determined by standards issued by the accreditation bodies of the respective country. For ISO standard audits, two relevant standards are crucial: ISO/IEC 17021 and ISO 19011. While ISO/IEC 17021 sets specific requirements for the conduct of external audits by auditing organizations, ISO 19011 serves as a general guide for auditing processes. This guide can also be used by companies that do not perform audits, for example, for internal audits or the assessment of suppliers as third parties. The ISO 19011 also provides guidance for assessing auditor competence on various subjects and answers questions about the competency assessment process. The conduct of external audits by independent accounting firms follows a similar approach to that established by the two relevant standards mentioned above. This makes it possible to compare the resulting findings of ISO-based MS audits. Many ISO standards are based on a so-called High-Level Structure (HLS, possibly supplementary ANNEX), which simplifies the use of multiple management systems within a company. The basic structure of this HL structure can be seen in Table 2.

Vol. 9, No. 03; 2024

ISSN: 2456-3676

Table 2 The high-level structure of international management systems

Informal part	Main chapters inclusive short description
1. Scope 2. Normative references 3. Terms and definitions	4. Context of the organization - Includes defining the scope of the ISMS, as well as identifying external and internal issues relevant to information security. 5. Leadership - Explains management's responsibilities in setting information security policy and commitment to improving the ISMS. 6. Planning - Includes the processes for assessing risks and opportunities and setting information security aims. 7. Support - Defines the required resources, competencies, awareness and communication measures as well as the documentation of the ISMS. 8. Operation - Describes the operational processes for managing risks and implementing plans to achieve information security objectives. 9. Performance evaluation - Concerns the monitoring and measurement of the effectiveness of the ISMS as well as the internal auditing and management review. 10. Improvement - Refers to taking measures to continuously improve information security and ISMS in general.

Source: Authors own elaboration based on ISO/IEC27001 HLS.

Note: The appendix (also called the Annex with 114 controls) of ISO/IEC 27001 contains the catalogue of security controls known as Annex A. This appendix provides a framework for the best practice security measures to be implemented in an information security management system. Controls are divided into different domains or categories, and each category addresses specific aspects of information security.

Each of these chapters contributes to establishing and maintaining an effective information security management system designed to ensure the classic protection objectives as well as confidentiality, integrity and availability of information. The supplementary requirement criteria for Critical Infrastructure operators according to ISO/IEC 27019:2020, the IT security catalog 1a and 1b, and the BSI requirements catalog for the deployment of attack detection systems are specific provisions which contribute indirectly to information security and cyber security. For appropriate and suitable comparability, these are aligned with the requirements of ANNEX A according to ISO/IEC 27001 and classified as specific security categories, see table 3.

Vol. 9, No. 03; 2024

ISSN: 2456-3676

Table 3. Overview of specific security categories

Security categories	Chapter in context of Scope of Applicability (SoA) according ISO/IEC 27001 and ANNEX A
Organization	4. Context of the organization 5. Leadership 6. Planning 7. Support 8. Operation 9. Performance evaluation 10. Improvement A.5* Information Security Policies A.6* Organization of information security
People & Assets	A.7* Human resource security A.8* Asset management A.9* Access control
Physical Security	A.11* Physical and Environmental Security
Operation security	A.10* Cryptography A.12* Operations security A.13* Communication security A.14* Security in development and support processes
Supplier relationship security	A.15* Supplier relationships
Risk Management and Incident Handling	A.16* Information Security Incident management A.17* Information Security Aspects of BCM
Compliance	A.18* Compliance

Source: Authors own elaboration based on ISO/IEC27001 HLS.

Note: * Specific requirements according to ISO/IEC 27019:2020, IT security catalogue 1a and 1b as well as the specifications catalogue according to BSI for the use of attack detection systems (systems for attack detection) were included.

Determine elements within this structure are consistent across all systems and therefore only need to be implemented once. Each individual chapter of the HLS has a specific and differentiated focus within each management system, whereupon the fulfillment of the requirements of each MS is based on this generic High Level Structure (HLS). Although there are differences in content between the various standards of management systems, each system follows a cyclical process of continuous improvement (for example based on the plan-implement-check-act cycle) including common requirements. The criteria utilized and examined in this research are summarized as follows:

Vol. 9, No. 03; 2024

ISSN: 2456-3676

- A risk-based approach is required for MS. The aim of this risk-based approach is to identify risks concisely and sustainably and to determine measures.
- Management commitment and involvement. Management systems based on ISO aim to improve the organization and related business processes in terms of the type of management system. This also includes precise planning and procurement of the necessary resources (including personnel and training, etc.), evaluating and improving the ISMS.
- An evaluation and improvement process is important to regularly evaluate the MS through a recurring assessment using KPI (Key Performance Indicators) measurement methods.

The requirements according to ISO/IEC 27001 must be met by the operators of critical and non-critical infrastructures and checked for conformity through external audits. During each audit, the auditors check the conformity of the measures established in the company against the regulatory requirements (legal, official, contractual) and identify non-conformities as well as recommendations with regard to the existing management system. Each audit includes targeted conformity checks on organizational, technical, personnel and physical measures take place, which are documented by the auditor or team of auditors during the certification process. The extent to which the established management system corresponds to or deviates from the normative requirements is specified and demonstrably recorded as findings.

The differentiation between the findings as serious or minor deviations is crucial. Since serious deficiencies result in an unsuccessful audit, minor deviations can be corrected by the next audit to ensure that the audited standards are adequately met. Recommendations in the context of an audit usually refer to suggestions or actions aimed at addressing identified and potential optimizations and improving the management system of the audited company. They are given by the auditor team after analyzing the management system, procedure or a specific process. Recommendations may include specific steps for improvements, strategic changes, or complementary change implementation of control mechanisms. The aim of these recommendations is to optimize the efficiency, effectiveness and compliance of the management system with the relevant standards and best practices.

3.2 Audit results of the evaluation of MS for critical and non-critical operators

The result of this database-based research can be seen in Figure 1 and 2, which shows the average number of NC and RC from CRITIS and Non-CRITIS operators. These Non-Conformities (NC) are assigned and presented according to chapters according to the HL structure of the audited ISO-based management system standards according to ISO/IEC 27001 and the associated ANNEX A.

Vol. 9, No. 03; 2024

ISSN: 2456-3676

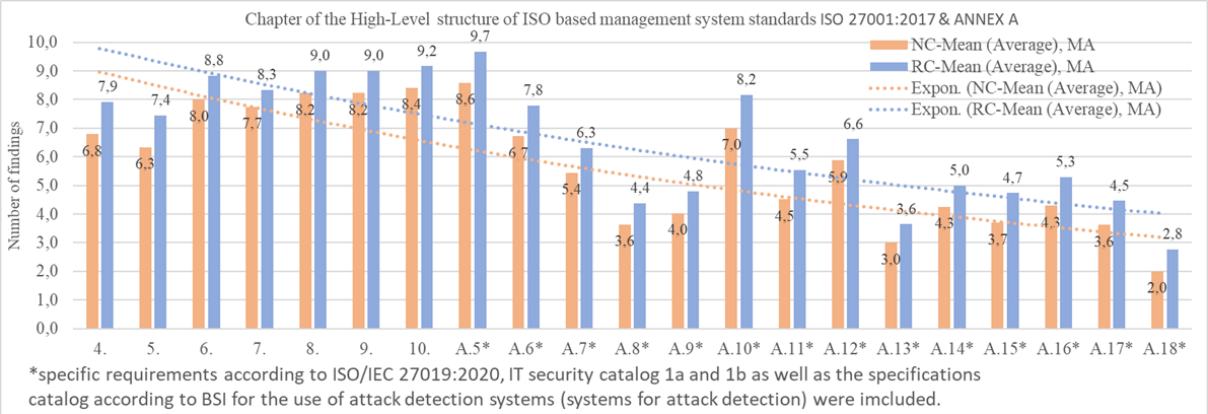

Figure 1 Number of non-conformities in external management system audits in 91 operators of critical infrastructure

Source: Authors own elaboration based on the results of own research.

The specific requirements are in accordance with the appropriate comparability for the operators of critical infrastructure to

- ISO/IEC 27019:2020,
- IT security catalogue 1a and 1b and
- catalogue of specifications according to BSI for the use of attack detection systems (systems for attack detection),

which added to ANNEX A of ISO/IEC 27001. These are classified and marked separately as specific security categories, as can be seen in Figure 2.

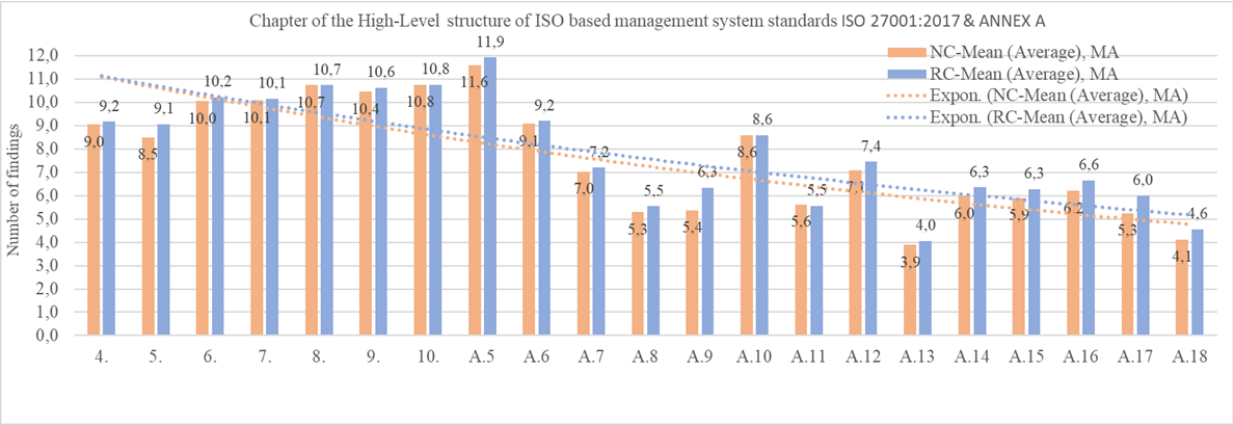

Figure 2 Number of non-conformities in external MS audits in 87 operators of Non-Critical Infrastructure

Source: Authors own elaboration based on the results of own research.

Vol. 9, No. 03; 2024

ISSN: 2456-3676

The average number of Non-conformities (NC) and Recommendations (RC) from operators of Critical Infrastructure (CRITIS) is lower than for operators of Non-Critical Infrastructure (Non-CRITIS). Furthermore, it can be concluded that it is in the

- Chapters for CRITIS: 6, 8, 9, 10, A.5*, A.6*, A.10*, A.12*, A.14 - A.17,
- Chapters for NON-CRITIS: 6-10, A.5, A.6, A.7, A.10, A.12, A.14 - A.17

There are a similar number of NC and RC versions. In some cases there are very focused chapters, such as in 6, 8, 9, 10, A.5, A.6, A.10, A.12 for operators of Critical Infrastructure and operators for Non- Critical Infrastructure. It is also clear that the average number of Non-Conformities (NC) and Recommendations (RC) is higher for operators of Critical Infrastructure and operators for Non- Critical Infrastructure in the HL structure. This confirms the first two hypotheses of this research. In the following will be represented the number of NC and RC in external management system audits in 178 organizations from 2019 to early 2024.

Table 4. Number of Non-Conformities and Recommendations in external management system audits in 178 organizations (2019 to early 2024)

Description	Operators of critical infrastructure		Operators of non-critical infrastructure	
	Value according to NC	Value according to RC	Value according to NC	Value according to RC
HLS Number from 2019 to early 2024	1.283	1.320	1.632	1.567
HLS Mean (Average):	8.224	8.461	10.461	10.044
ANNEX A Number from 2019 to early 2024	3.244	3.634	4.299	4.375
ANNEX A Mean (Average):	4.742	5.314	6.285	6.396
Legend: NC - Non-Conformities and RC - Recommendations				

Source: Authors own elaboration based on the results of own research.

As a result, there are overall more non-conformities in areas within Annex A than in the higher-level structural chapters. This also confirms hypothesis 3.

The table 5 shows the most common measures of dispersion for metric variables such as the standard deviation, variance, population standard deviation, variance (population standard) and the mean value of Non-Conformities (NC) and Recommendations (RC) from operators of critical infrastructure and operators of non-critical infrastructure.

Vol. 9, No. 03; 2024

ISSN: 2456-3676

Table 5. Number of NC and RC in external management system audits in 178 organizations (2019 to early 2024)

Mathematical expression	Operators of critical infrastructure		Operators of non-critical infrastructure	
	Value according to NC	Value according to RC	Value according to NC	Value according to RC
Sample Standard Deviation, s	2.558	2.774	2.700	2.802
Variance (Sample Standard), s.2	7.541	8.763	8.057	8.712
Population Standard Deviation, σ	2.503	2.715	2.644	2.746
Variance (Population Standard), σ2	7.186	8.357	7.702	8.358
Mean (Average):	5.733	6.612	7.644	7.918

Source: Authors own elaboration based on the results of own research.

This shows that the NC- critical infrastructure mean is 5.733 and the RC- critical infrastructure mean is 6.612. Based on this result and despite a relatively medium standard deviation of 2.558 NC and 2.774 RC in the critical infrastructure, the results show that the audit findings in the main chapters 6, 7, 8, 9, 10, A.5*, A.6*, A.10*, A.12* is above the average compared to the other chapters.

In comparison, the NC and RC mean values are higher in of non- critical infrastructure Non-CRITIS. Additionally, for both operators, it is important to highlight Chapter 6 of the HLS, which necessitates a clear-cut approach to risk management as part of the management system. This also confirms hypothesis 1 to 3. The results can definitely be attributed to various factors:

- Regulatory requirements: operators of critical infrastructure are generally subject to additional legal and regulatory requirements in accordance with ISO/IEC 27019:2020, IT security catalog 1a and 1b, specifications catalog according to BSI - System for Attack Detection). The regular audits are carried out by the N3I auditors from independent bodies. This leads to greater urgency and motivation to identify and close compliance gaps.
- Risk awareness: Due to the potentially serious impact of a critical infrastructure outage or security incident, risk awareness among operators for critical infrastructure is higher, leading to more proactive processes for risk management and business compliance.
- Internal control systems: Critical infrastructure operators often implement specific internal control systems and processes to ensure compliance, which are constantly monitored and

Vol. 9, No. 03; 2024

ISSN: 2456-3676

updated to risk, monitoring and logging processes. The result is a lower probability of non-compliance and improvements.

- Continuous Improvement: There is often a heightened corporate risk-taking culture in the critical infrastructure space, where identified deficiencies and improvements are addressed quickly to maintain and strengthen compliance, leading to continuous improvement.
- Investing in security, public pressure and reputation: critical infrastructure operators are aware of the potential consequences to the public if their systems fail. The high priority of security at critical infrastructure often leads to greater investments in security measures, personnel and technology. This helps avoid non-compliance.

4. Conclusion

In summary, it can be stated that all hypotheses could be answered positively for both Critical Infrastructure and Non-Critical Infrastructure operators. Among the organizational samples employed in this research, there was a higher tendency for non-conformities in certain areas of the HLS chapters during external audits than in others. The Annex A of ISO/IEC 27001 contains the catalog of security controls, which was supplemented for Critical Infrastructure operators with specific security requirements to allow for an appropriate and suitable comparison with Non- Critical Infrastructure operators. Since operators usually have to comply with additional legal and regulatory requirements and undergo regular audits by N3I auditors, this illustrates an increased motivation to identify and close compliance gaps.

The various chapters 6, 8, 9, 10, A.5, A.6, A.10, A.12 for Critical and Non-Critical Infrastructure operators showed a heightened tendency for non-conformities and recommendations for improvement. These chapters particularly focus on aspects of the management involvement of leadership, the operation of the MS and the associated business processes, the performance MS evaluation, continuous improvement, cryptography, and operational security.

The risk management aspect discussed in Chapter 6 of HLS is a focal requirement, often leading to NC and RC, which may indicate the necessity of using a standardized risk management process for IS and CS. This is also underscored by the research in hypotheses 1 to 3, which shows that the integration of Risk Management (RM) into the MS within the organization-wide RM process (if present in the organization) is beneficial for businesses. Recognizing the organizational structures and decision-making processes, global risks must be more closely integrated into the existing risk management process for operators of critical and non-critical infrastructure.

A more strategic evaluation of the management system's performance also appears to be beneficial. Fundamentally, this seems to be due to the transparency of the results and improvements in organizational processes brought about by external audits, which are treated with special attention at the chief level and seen as an opportunity.

Vol. 9, No. 03; 2024

ISSN: 2456-3676

In conclusion, it should be mentioned that no distinction is made between the various industries and the management standards used, and therefore it will be a partial objective of the next research. Here, the topics should be analyzed based on a sample to gain a more detailed insight into the special characteristics of the industries and the management system controls used.

References

Coppolino, L., D'Antonio, S., Formicola, V., Romano, L. (2011). Integration of a System for Critical Infrastructure Protection with the OSSIM SIEM Platform: A dam case study. In: Flammini, F., Bologna, S., Vittorini, V. (eds) Computer Safety, Reliability, and Security. SAFECOMP 2011. Lecture Notes in Computer Science, vol 6894. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-24270-0_15.

Culot, G., Nassimbeni, G., Podrecca, M. and Sartor, M. (2021), "The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda", The TQM Journal, Vol. 33 No. 7, pp. 76-105. https://doi.org/10.1108/TQM-09-2020-0202

DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. pp. 1-35. https://eur-lex.europa.eu/eli/dir/2022/2557/oj.

Enny Susilowati Mardjono, & Yahn-Shir Chen. (2020). Earning Management and the Effect Characteristics of Audit Committee, Independent Commissioners: Evidence from Indonesia. International Journal of Business and Society, 21(2), 569-587. https://doi.org/10.33736/ijbs.3272.2020.

Febriana, L.,Wardayati, S. M. & Prasetyo, W. (2017). The Effect of Internal Control Factors on the Accountability of the Auditor at the Inspectirate of Jombang District. Jurnal Dinamika Akuntansi, 9(2), 166-175. https://doi.org/10.15294/jda.v9i2.9308.

Foglietta, C. and Panzieri, S. (2020), 'Resilience in Critical Infrastructures: The Role of Modelling and Simulation', Issues on Risk Analysis for Critical Infrastructure Protection [Working Title]. IntechOpen, Nov. 19, 2020. doi: 10.5772/intechopen.94506.

Gao, L., Aguiar-Moya, J. P., & Zhang, Z. (2011). Performance Modeling of Infrastructure Condition Data with Maintenance Intervention. Transportation Research Record, 2225(1), 109-116. https://doi.org/10.3141/2225-12.

Kure, Halima Ibrahim, Shareeful Islam, and Mohammad Abdur Razzaque. 2018. "An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System" Applied Sciences 8, no. 6: 898. https://doi.org/10.3390/app8060898.

Lampe, G., (2021), "Study on Information Security Challenges in Digital Transformation", 37th IBIMA Conference: 30-31 May 2021, Cordoba, Spain, ISBN: 978-0-9998551-6-4, ISSN: 2767-9640, pp. 438-466.

Lampe, G.S., Olaru, M., Maftei, M. and Ilie, C., 2021. Study on Information Security Management System and Cyber Security Strategy in the context of SCRUM. In: R. Pamfilie, V. Dinu, L. Tăchiciu, D. Pleșea, C. Vasiliu eds. 2021. 7th BASIQ International Conference on New Trends in Sustainable Business and Consumption. Foggia, Italy, 3-5 June 2021. Bucharest: ASE, pp. 811-819, DOI: 10.24818/BASIQ/2021/07/102.

Vol. 9, No. 03; 2024

ISSN: 2456-3676

Lampe, G.S., Olaru, M., Fogoros, T.E. and Massner, S.,2022. Critical Success Factor for Integration of Cyber Security in Context of Managed Services. In: R. Pamfilie, V. Dinu, C. Vasiliu, D. Pleșea, L. Tăchiciu eds. 2022. 8th BASIQ International Conference on New Trends in Sustainable Business and Consumption. Graz, Austria, 25-27 May 2022. Bucharest: ASE, pp. 911-919. DOI: 10.24818/BASIQ/2022/08/098.

Manaf, N. A. (2010). The impact of performance audit: The New Zealand experience. Master Thesis, Victoria University of Wellington. 1-11.

Morin, D. (2001). Influence of value for money audit on public administrations: looking beyond appearances. Financial Accountability & Management, 17(2), 99-117.

Morin-Danielle. (2003). Controllers or catalysts for change and improvement: would the real value for money auditors please stand up? Managerial Auditing Journal, 18(1), 19-30.

Morins, D. (2004). Measuring the impact of value-for-money audits: a model for surveying audited managers. Canadian Public Administration, 47(2), 141-164.

Nugraheni et al. (2021). Symbolic interaction of internal auditor in the implementation of consultation activities. IOP Conf. Ser.: Earth Environ. Sci. 724 012098, 1-6. https://dx.doi.org/10.1088/1755-1315/724/1/012098.

Olaoye, F. O., & Adedeji, A. Q. (2019). Performance Audit and Public Sector Budgetary Efficiency in Southwest Nigeria. Journal of Accounting, Business and Finance Research, 5(1), 17–22. https://doi.org/10.20448/2002.51.17.22.

Olatunji, O. C., & Adekola, D. R. (2017). The Roles of Auditors in Fraud Detection and Prevention in Nigeria Deposit Money Banks: Evidence from Southwest. European Scientific Journal, ESJ, 13(31), 290. https://doi.org/10.19044/esj.2017.v13n31p290.

Ray Bernard, Information Lifecycle Security Risk Assessment: A tool for closing security gaps, Computers & Security, Volume 26, Issue 1, 2007, Pages 26-30, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2006.12.005.

Reichborns, K., K. (2013). Political accountability and performance audit: The case of the auditor general in Norway. Public Administration, 91(3), 680-695.

Reichborn-Kjennerud, K., & Johnsen, Å. (2011). Auditors‘ understanding of evidence: A performance audit of an urban development programme. Evaluation, 17(3), 217-231.

Reichborn-Kjennerud, K. (2015). Resistance to control—Norwegian ministries‘ and agencies‘ reactions to performance audit. Public Organization Review, 15(1), 17-32.

Uchenna D Ani and Jeremy D McK. Watson and Jason R. C. Nurse and Al Cook and Carsten Maple (2019). A Review of Critical Infrastructure Protection Approaches: Improving Security through Responsiveness to the Dynamic Modelling Landscape. Cryptography and Security (cs.CR); Networking and Internet Architecture (cs.NI); Systems and Control (eess. SY), 1–16. https://doi.org/10.48550/arXiv.1904.01551.

World Economic Forum, 2024. The Global Risks Report 2024. 19th ed. [online] The Global Risks Report 2024, Geneva: World Economic Forum. Available at: <https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf> [Accessed 17 Jan. 2024].