Model of formalized information security audit of an organization with a critical infrastructure facility for compliance with international security standards

Nataliia Lishchyna[1,†], Valerii Lishchyna[1,†], Lesia Kozubtsova[2,*,†], Igor Kozubtsov[1,†] and Andrii Yashchuk[1,†]

[1] *Lutsk National Technical University, Lvivska Street 75, 43018 Lutsk, Ukraine*
[2] *Heroiv Krut Military Institute of Telecommunications and Informatization, Knyaziv Ostrozkykh 45/1, 01011 Kyiv, Ukraine*

Abstract

The article emphasizes the importance of conducting information security audits for information systems of critical infrastructure organizations. Effective protection is ensured by aligning security systems with international standards. The audit monitors and assesses compliance but remains effective only when performed regularly by trained specialists. Due to the routine nature of audits and wartime constraints, such as power outages and loss of communication, AI-based methods are often impractical. Therefore, the authors propose a temporary solution using formalized security assessment criteria with clear indicators for objective verification. The study develops a methodology for conducting audits aligned with international standards, addressing the lack of practical guidance in existing ones. It also analyzes global regulatory documents to identify typical management approaches and proposes an adaptable checklist-based methodology covering 10 key information security areas, particularly useful for organizations operating under wartime conditions.

Keywords

Model, audit, information security, international standards, control, indicators, methodology.

1. Introduction

Today, information systems play a key role in ensuring the efficiency of both commercial and state enterprises. The widespread use of information systems for searching, storing, processing, and transmitting information makes the problem of their protection particularly urgent, especially given the global trend of increasing information attacks that cause significant financial and material losses. To effectively protect against such attacks, companies need an objective assessment of the information security level of their systems, which is achieved through an information security audit.

As a rule, audits are conducted by external consulting companies specializing in information security. The initiative for carrying out such procedures may come from enterprise management, automation services, or information security departments. In some cases, audits are also required by insurance companies or regulatory authorities. Security audits are performed by groups of experts, whose number and composition depend on the goals, objectives, and complexity of the assessed system.

However, in state institutions and critical infrastructure facilities with high confidentiality requirements, the involvement of external audit companies is prohibited. In such circumstances, organizations must develop their own audit methodologies and engage specialists with the appropriate level of access. This limitation significantly restricts the use of standard solutions, especially under wartime conditions in Ukraine.

AIT&AIS'2025: International Scientific Workshop on Applied Information Technologies and Artificial Intelligence Systems, December 18–19 2025, Chernivtsi, Ukraine
[1,*] Corresponding author.
[†] These authors contributed equally.
lischyna@gmail.com (N. Lishchyna); lvaleriy@gmail.com (V. Lishchyna); lesia.kozubtsova@viti.edu.ua (L. Kozubtsova); kozubtsov@gmail.com (I. Kozubtsov); xxxxandyxxxx@gmail.com (A. Yashchuk)
00000-0002-5200-536X (N. Lishchyna); 0000-0002-2371-3850 (V. Lishchyna); 0000-0002-7866-8575 (L. Kozubtsova); 0000-0002-7309-4365 (I. Kozubtsov); 0000-0003-4872-7949 (A. Yashchuk)

The owner and/or manager of a critical infrastructure facility is legally obliged to organize and conduct an independent information security audit in compliance with Ukrainian legislation in the field of information protection and cybersecurity. These requirements are defined by the National Security Strategy of Ukraine, the Concept for the Development of the Security and Defense Sector of Ukraine [1, p. 33], the Law of Ukraine "On the Basic Principles of Cybersecurity of Ukraine" [2], the Cybersecurity Strategy of Ukraine [3], and the Resolution of the National Security and Defense Council of Ukraine [4].

Therefore, addressing the scientific problem of conducting a critical infrastructure protection (CIP) audit in accordance with the general requirements of the Cabinet of Ministers of Ukraine Resolution of June 19, 2019, No. 518 "On Approval of General Requirements for Cyber Protection of Critical Infrastructure" [5] is highly relevant today.

1.1. Problem statement

An information security (IS) audit, as a systemic activity, is aimed at monitoring and verifying the state of the IS of a protected object (in particular, an organization), as well as assessing the adequacy of the applied means and methods of information protection in accordance with existing threats. The foundation of effective enterprise protection lies in the timely configuration of the security system and the periodic work of responsible personnel involved in the IS audit [6].

Therefore, the general task of an IS audit is to verify the compliance of the protection system with a set of criteria that define the security requirements. The auditor's work is highly meticulous and often routine, which makes the process in need of simplification. In this context, there is a need for a scientifically grounded definition and formalization of a set of criteria that reflect the security level of the object, along with the identification of indicators that enable objective verification procedures. These criteria should be clearly defined and, as far as possible, measurable [7].

It is worth noting that, at the early stage of establishing information protection systems and cybersecurity, the formation of such systems, which were previously unknown, proved to be an extremely complex task.

1.2. Literature review. Analysis of recent scientific research and publications

At the initial stage of addressing information security (IS) and cybersecurity problems, scientists worldwide faced the difficult task of justifying the choice of evaluation criteria, which needed to be clearly defined and as measurable as possible. The development of a unified approach to building a methodology for assessing organizational cybersecurity began with debates caused by the absence of a consistent terminological framework.

The authors of [8] proposed non-standard approaches to developing a methodology for assessing the cybersecurity of organizational communication systems. The urgent demand for such research led to the creation of a formalized methodology for assessing the cybersecurity of information and telecommunication systems [9]. However, in practice, the process proved to be more complex. The existence of zero-day threats introduced unpredictability, making standard methodologies without a well-justified choice of evaluation criteria insufficiently objective, particularly when they did not assess the effectiveness of implemented cybersecurity measures [10]. This gap highlighted the need for methodologies focused on evaluating the effectiveness of cybersecurity measures, which themselves required further development [11].

At the same time, scientific research was conducted under state orders [12] to develop audit methodologies for critical infrastructure facilities. These methodologies, even after significant simplifications [13], remained complex and posed difficulties for inexperienced auditors in compiling a comprehensive list of checks.

As separate initiatives, it is worth highlighting [14], which substantiated the need for technical audits of information and telecommunication systems at enterprises. This work outlined audit procedures and vulnerability testing for systems where restricted-access information is not

processed. The proposed audit technology relied primarily on active penetration testing of IT infrastructures.

The study [15] examined the problem of organizing internal audits in the realities of the Ukrainian economy. It was determined that traditional audit methods, based on selective analysis and retrospective control, fail to provide sufficient efficiency in the modern environment. Such audits are characterized by large data volumes, and conventional approaches relying on manual big data collection and periodic checks demonstrate inadequate effectiveness in digital systems.

The revolution in cybersecurity auditing began with the introduction of artificial intelligence (AI) automation [16]. Subsequent research has focused on the potential of AI in auditing and managing cybersecurity risks in the context of digital transformation [17]. The integration of AI technologies enables automatic anomaly detection, proactive risk assessment, generation of recommendations, and analysis of large volumes of both structured and unstructured data (event logs, network traffic, text reports, etc.). According to [18], the use of AI in cybersecurity audits will significantly enhance transparency and accountability, particularly in peacetime.

1.3. Highlighting understudied aspects

The analysis of recent research and publications has shown that it is impossible to define universal formalized indicators and criteria for conducting audits that would be applicable to all tasks and types of audits in peacetime. Moreover, the use of artificial intelligence in audits of information security and cybersecurity at critical infrastructure facilities during wartime, at least in Ukraine, is unacceptable due to frequent force majeure circumstances, such as power outages, loss of communications, and lack of Internet access.

2. Purpose of the article

The purpose of this article is to test the process of forming a formalized audit methodology and practice-oriented instructions for conducting audits of an organization's information security in compliance with standards and regulatory requirements. Within the framework of the proposed methodology, it is possible to develop similar instructions for any chosen standard.

2.1. Research objectives (goals)

To achieve this purpose, the following objectives are set: 1. To analyze recent research and publications on the problem under study. 2. To present and explain the author's own research results.

3. Research methods

3.1. Research tools

To solve the defined tasks, theoretical research methods were applied, namely: analysis and synthesis of scientific literature on the subject; analytical and comparative analysis to assess the novelty of the study; synthesis and generalization to substantiate the methodological foundations of the research; generalization for the formulation of conclusions and recommendations for further studies.

3.2. Reliability and accuracy of results

The reliability of the obtained results is ensured by the correct application of mathematical tools and research methods. A set of scientific methods, comprehensively substantiated and integrated into a single system, provided for the reliability and accuracy of the scientific outcomes in accordance with the methodology of scientific research.

3.3. Methodological basis of the study

The methodological basis of the study is formed by the procedures for selecting the audit object. The objects of an IS audit can include a wide range of entities and processes [19], such as: automated or information systems and their individual components; organizational and management processes; technical means; business procedures; the overall activities of the enterprise.

From the perspective of audit form, an IS audit may be: organizational and regulatory [20], where the subject of analysis is measures and regulatory documents ensuring IS; technical, where the subject of analysis is the technical means of information processing.

The set of IS risk analysis methods is based on two models:

1. Compliance-based model – risk is determined by comparing the compliance of the protected object with IS requirements derived from standards, regulatory acts, and system operating conditions.
2. Probability-damage model – risk is determined by assessing the probabilities of threats and attacks, as well as the magnitude of potential material damage.

Conceptually, IS audit models can be grouped into three practical and three theoretical approaches.

Practical approaches: audit based on risk analysis; audit based on IS standards analysis; audit incorporating experimental studies of the object.

Theoretical approaches: audit based on process modeling; audit based on an assessment model; audit using the maturity model.

One of the most widespread methods is the standards-based audit, since standards provide a set of requirements and recommendations for IS, grounded in professional experience, and serve as regulatory references in the professional community.

IS audits can be conducted for compliance with international standards such as ISO/IEC TS 33030:2017 [21], ISO/IEC 21827:2008, and ISO/IEC 27001:2022 [22], depending on the organization's tasks. In Ukraine, the Resolution of the Cabinet of Ministers of Ukraine of 19.06.2019 No. 518 [5] defines the general requirements for the cyber protection of critical infrastructure facilities. However, practice has shown that without a clear understanding of cybersecurity structures and IS standards, it is impossible to conduct audits effectively [5]. The accumulated knowledge has laid the groundwork for understanding the functional features of intelligent internal audit systems [23].

The ISO/IEC 27002:2022 standard [24] is a key document that defines the main directions of IS management in organizations and often serves as the foundation for audits. Notably, research such as [25] examined the benefits of cross-implementation of cybersecurity audit standards. However, as this approach falls outside the scope of the present study, it is not considered further.

4. Research results

Returning to international standards, it should be noted that the vast majority of basic standards in the field of IS protection and IS management at enterprises have a predominantly descriptive nature. They provide sets of recommended management actions but generally lack: criteria for the completeness of management actions; discrete and unambiguously interpretable indicators of feasibility and effectiveness; methods for achieving the intended results; clear instructions for implementing compliance checks.

The main difficulties in conducting an IS audit for compliance with standards stem from the absence of a clear and consistent audit methodology, as emphasized in [8]. When auditing IS, subjectivity should be minimized, since the reliability of audit results increases with their degree of formalization. Nevertheless, it is impossible to completely eliminate subjectivity.

The formalization of audit processes is a relevant but still understudied research direction. Attempts at formalization have been made, primarily in relation to individual aspects of audits,

using the so-called “audit approach based on the reference model” [12]. The task of formalization is to ensure the repeatability and independence of audit procedures and results.

One of the most effective practices is the development of checklists (control charts) that define the sequence of audit procedures, the processes being verified, and their discrete indicators.

To illustrate, let us consider the audit tasks and actions when assessing an organization’s IS compliance with the ISO/IEC 27002:2022 standard. This standard defines security requirements based on: IS risk assessment; regulatory requirements; specific organizational principles shaped by the enterprise’s environment.

The standard prioritizes protection of three categories of information: personal data; organizational credentials; intellectual property.

The set of protective measures includes: the presence of IS policies; distribution of responsibilities for IS; staff training on IS issues; procedures for reporting IS incidents; business continuity management.

The protection of personal data and privacy is of particular importance for a modern society [26]. Based on public needs, protective measures must be applied to each information category. Conversely, each measure should be designed to cover all categories of information.

To systematize these relationships, a generalized protection matrix (Table 1) is proposed. It defines 15 protection functions (F_{11}, …, F_{53}), each of which can be assessed by the degree of compliance with the defined requirements.

Table 1
Generalized protection matrix

Activities	Information Categories		
	Personal Data	Organization Credentials	Intellectual Property
IS Policies	F_{11}	F_{12}	F_{13}
Segmentation of Responsibilities	F_{21}	F_{22}	F_{23}
Staff Training	F_{31}	F_{32}	F_{33}
Incident Reporting	F_{41}	F_{42}	F_{43}
Business Continuity Management	F_{51}	F_{52}	F_{53}

The ISO/IEC 17799:2005 standard divides IS management processes into ten key areas [27]:

1. Security policy.
2. Information security organization.
3. Asset management.
4. Human resource security.
5. Physical and environmental security.
6. Communications and operations management.
7. Information systems acquisition, development, and maintenance.
8. Business continuity management.
9. Information security incident management.
10. Compliance.

The objectives and controls specified in ISO/IEC 17799:2005 are designed to address requirements identified through risk assessment. This standard serves as a general framework and provides practical guidance for developing organizational security standards and implementing effective IS management practices.

The auditor's direct actions are aimed at verifying the compliance of the facility's security measures across these ten areas. Such checks must be carried out using the most objective and repeatable methods available. The developed author's model of audit control, structured within the selected areas, is presented in Figure 1.

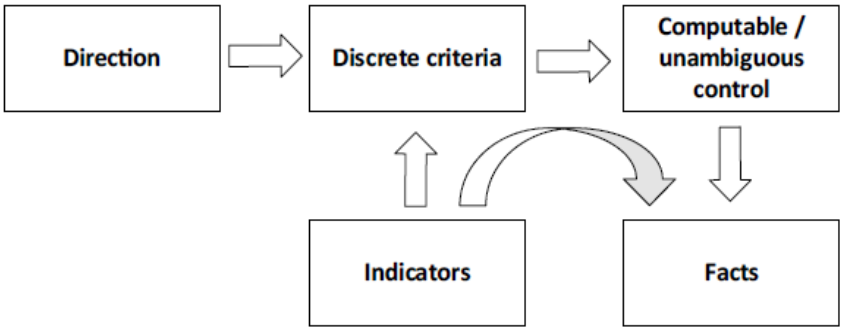

Figure 1: Audit Control Model.

The general scheme of the process data interaction model for information security audit management within the framework of the implementation of the information security management method based on dynamic expert decision support systems is presented in Figure 2.

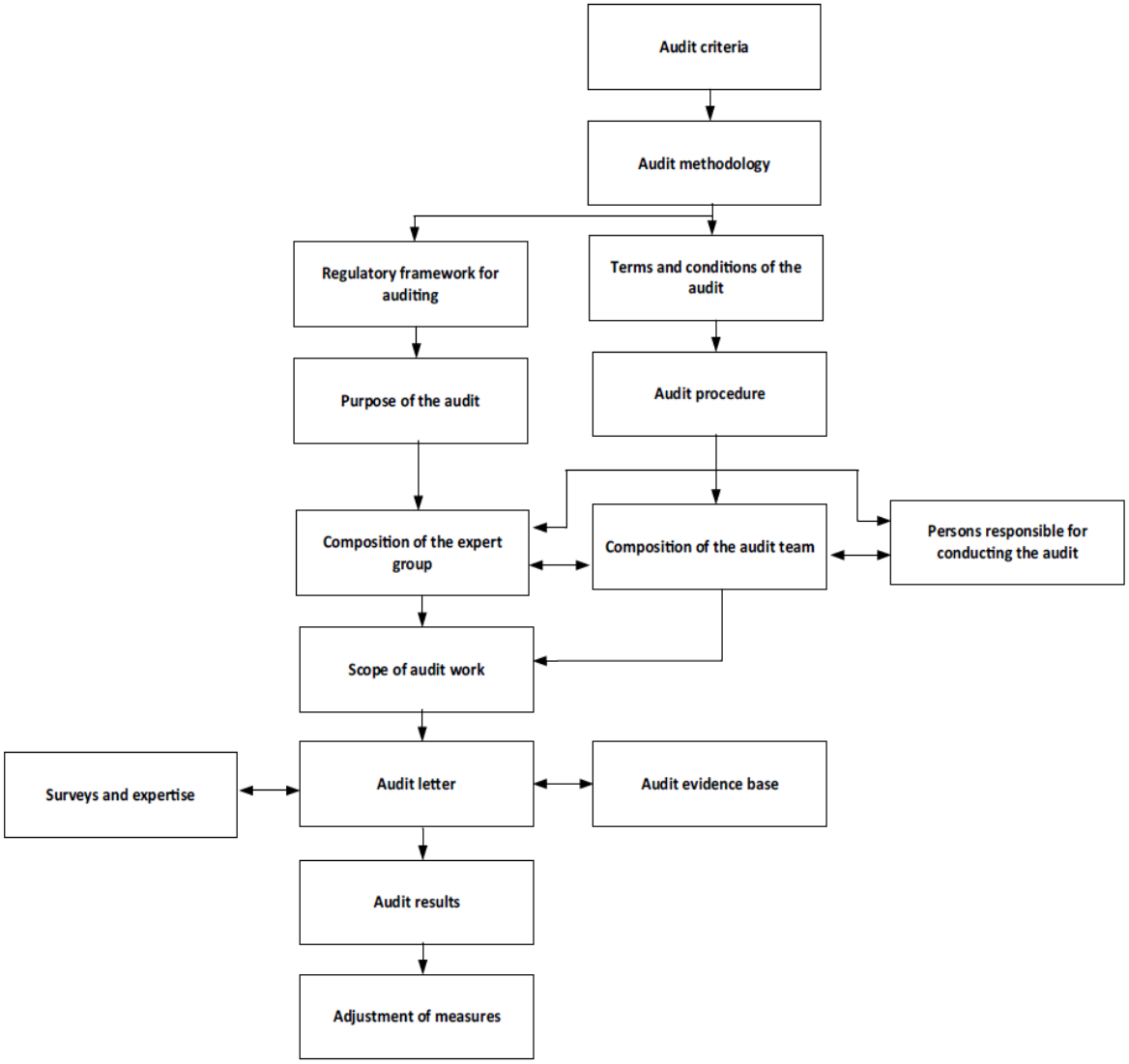

Figure 2: Diagram of the data interaction model of the information security audit management process.

According to the proposed model, the auditor: determines the facts related to the audited procedures and the applied methods of information protection; collects evidence (confirmations) of these facts; uses exclusively objective, discrete criteria; records the results of the audit as unambiguously interpreted or calculated indicators.

The system of objective indicators and audit control criteria is fundamental. For this purpose, auditors can, in particular, be guided by the ISO/IEC 27001:2022 standard. Audit procedures within the ISO/IEC 2700x standards system, implemented in the PDCA cycle, constitute an independent concept and are not considered in this study.

Table 2 provides an example of management objectives and measures selected from the ISO/IEC 27001:2022 standard for the area "Information Security Policy" [22].

Table 2
Objectives and measures of information security policy management

A.5.1.1	Information security policy documentation	The information security policy must be approved by management, issued, and communicated to all employees of the organization, as well as to third-party organizations
A.5.1.2	Review of the information security policy	The organization's information security policy must be analyzed and revised at specified intervals, or when significant changes occur in the characteristics of security objectives

The information provided is decisive for assessing compliance, since it specifies the facts that the auditor must confirm or refute. However, it does not contain verification criteria. Therefore, there is a need to create a formalized scheme and/or algorithm of audit actions based on discrete criteria and clearly defined objective indicators.

Such a model can be represented as checklists consisting of clearly formulated questions, to which only explicit, unambiguous answers are possible, thus excluding subjectivity.

To build these checklists, we use the objectives, measures, and requirements formulated in the ISO/IEC 27001:2022 standard.

As an example, in the area of "Information Security Policy" the standard emphasizes the responsibility of the organization's top management for participation in IS-related decisions in accordance with business objectives, laws, and regulatory requirements.

The current legislation of Ukraine does not establish direct requirements for the form or content of IS policies. As a result, organizations demonstrate diverse approaches to their development. In contrast, the ISO/IEC 17799:2005 standard defines minimum requirements for IS policy content, although a detailed review is beyond the scope of this study. Based on these requirements and instructions, the auditor compiles a set of questions forming a checklist, to which answers are sought in the form of evidence and supporting facts during the audit process.

Requirements for evaluation criteria. The evaluation criteria must be objective, discrete, calculable, measurable.

Requirements for checklist questions: answers must be clear and unambiguous; answers must be verifiable; questions must not allow for subjective reasoning.

Table 3 presents a sample checklist for auditing in the area of "Information Security Policy." The proposed checklist can be expanded by the auditor depending on specific tasks.

The principles of checklist construction are as follows: all questions are grouped into levels (in this case, three); if the answer to a higher-level (first-level) question is negative, there is no need to continue with the lower-level questions; alternative models of level representation for security assessment in the audit process are also described in [27].

As shown in Table 3, all collected confirmations are expressed either in discrete values (yes/no, present/absent, compliant/non-compliant, etc.) or in calculated indicators (average test score, percentage of employees familiarized or trained, etc.). It is important not to confuse verification of employees' knowledge of a specific organizational IS policy (as an internal regulatory document) with testing their knowledge of the general theory and methodology of information protection.

Table 3
Auditor's work checklist

No	Level	Control indicator question	Answer		Method of confirmation
			Discrete	Calculated	
1	1	Is there an information security policy as a formal document?	Yes / No	–	Availability of the document
2	2	Has the security policy been formally approved by management?	Yes / No	–	Presence of requisites, signatures, official seal
	2	Is the security policy publicly available, including to third-party contractors?	Yes / No	–	(a) Place of publication; (b) Method of access
	...	...	...	...	...
N	1	Have employees received training on information security?	–	% of trained employees	Availability of training certificates, qualification and retraining documents

The following principles for compiling checklists can be formulated:

1. The fulfillment of each requirement of a regulatory document is determined by a control indicator.
2. Each control indicator appears in the form of an extremely clear, unambiguously interpreted question that provides for an unambiguous objective answer.
3. The answer to the question can be either discrete or in measurable, calculated values.
4. All questions that form control indicators are divided into levels.
5. Questions of the first (higher) level globally determine the facts of the fulfillment of the requirements.
6. Questions of the second and subsequent (lower) levels detail the degree of fulfillment of the requirements and characterize the level of protection.
7. The auditor collects answers to questions to confirm the facts.
8. With negative answers to questions of the upper levels, there is no point in checking statements on questions of the lower levels.
9. The quality of the formulations of control questions is determined by their objectivity, which is expressed in The indisputability of the answers even from the standpoint of third-party interest.

In the general case, based on the stated principle of checklist formation, each question (indicator) Si is described as the following function (1):

$$S_i(j)=\{X_i|Z_i\}, \quad (1)$$

where i – the question number, j – the question level, X – the discrete value of the answer (1 – "yes", "fulfilled", "present"; 0 – "no", "not fulfilled", "absent");

Z – the calculated value of the answer (expressed in fractions, percentages, or other units, e.g.: 1 – "fully satisfied", 0.75 – "mostly satisfied", 0.5 – "partially satisfied", 0.25 – "to a lesser extent", 0 – "not satisfied").

For first-level controls, it is advisable to use only questions with discrete answers.

The audit requirements are defined as follows: $S_i(1) = 1$ compliance with 100% of the first-level criteria; achievement of a minimum pre-defined performance threshold for the second and subsequent levels.

The thresholds for minimum performance are set as:

1. For the second level: at least 80% of the questions must be answered positively.
2. For the third level: at least 60% of the questions must be answered positively.

When preparing for the audit, checklists must be developed for all ten areas defined in the standard. Each question $S_i(n)$ is mapped to the corresponding function(s) F_{11}, …, F_{53}, forming a correspondence matrix (Table 4). To ensure the maximum connectivity between indicators and functions, the total number of completed measures is calculated along the rows (t) and columns (k) of the matrix, which reflects compliance both horizontally and vertically.

Table 4
Matrix of correspondence of protection functions according to checklists

	F_{11}	...	...	...	F_{53}	Together
$S_1(1)$	+					$t_1(1)$
$S_i(1)$		+	+			...
...	...	...	...	...	...	...
$S_i(2)$			+			...
...	...	...	...	...	...	...
$S_i(3)$	+					$t_1(1)$
Together	k_1	...	...	...	k_{15}	–

The sums of all responses at each level are calculated using formula (2):

$$C_N=\sum_{i=1}^{n} t_i(j), \quad (2)$$

where j – the current level.

The number of correspondences between answers and functions (3) is calculated:

$$D_N=\sum_{i=1}^{n} S_i(j). \quad (3)$$

The relevance of the compiled model is evaluated according to the principle of homogeneity, i.e., the obtained values of C_N and D_N should not differ significantly from each other. For the case

with 15 functions F_{11}, ..., F_{53}, the value of C_N is expected to lie approximately within the range of 3-5.

During the verification process, the auditor may also include additional measures in the checklists to assess the adequacy and effectiveness of information protection mechanisms, or organize them as part of a separate security research program. Such measures may include tests of the organizational structure's resistance to information-technical influences, and information-psychological influences.

While the assessment of resistance to information-technical influences is carried out within the framework of a technical and instrumental audit, the assessment of resistance to information-psychological influences can serve as a useful complement to the documentary audit. It helps identify the practical resilience of the organization's staff to information security threats.

Such test measures can be developed by the auditor, taking into account structural models of socio-psychological threats to information security.

5. Conclusions

Thus, an information security audit is currently one of the most effective tools for obtaining an independent and objective assessment of the enterprise's security level against information threats. Moreover, audit results form the basis for developing an organization's information security strategy. It should be emphasized that an audit is not a one-time procedure but must be conducted on a regular and systematic basis. Only under this condition will the audit produce real results and contribute to improving the company's overall level of information security.g channels, and creating a connection graph. The results are stored in the database for future use.

The proposed audit method is based on the formalization of the protection matrix and the development of objective checklists. The principles for compiling such checklists and assessing their relevance have been defined. An IS audit conducted according to the described model provides objective, repeatable, and unambiguous results, while also allowing the identification of weaknesses in the protection system and the development of recommendations for improving organizational security. Therefore, the application of this model is particularly advisable for audits of state institutions and critical infrastructure in Ukraine.

To enhance information security, it is recommended that government agencies in Ukraine conduct audits of critical infrastructure facilities in accordance with the PDCA (Plan–Do–Check–Act) cycle. The influence of audit frequency on the level of compliance is illustrated in Figure 3.

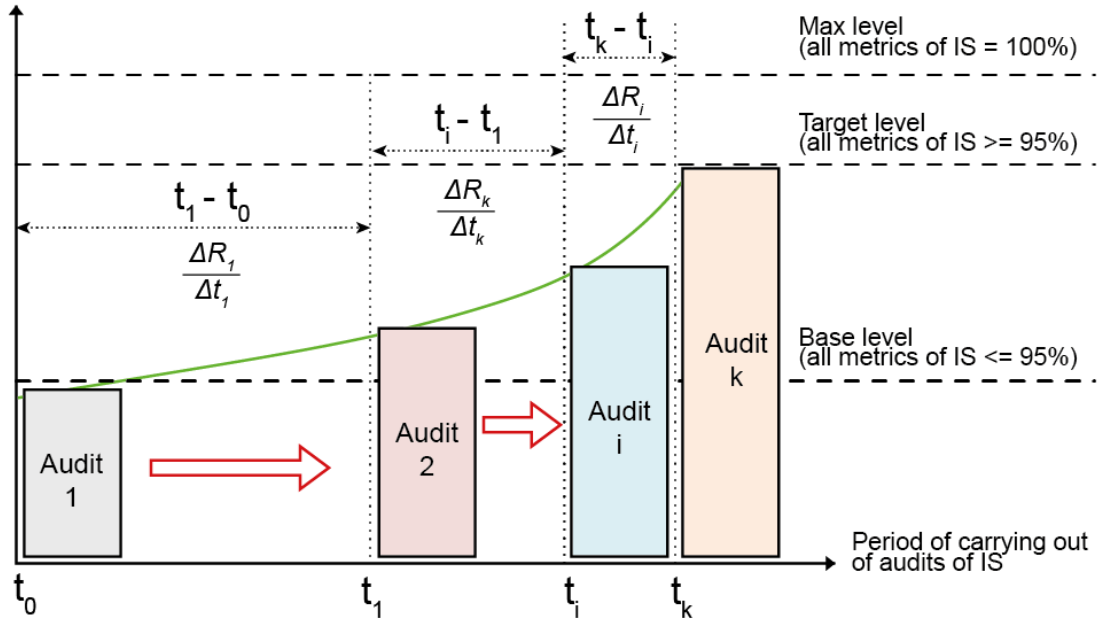

Figure 3: Influence of audit frequency on the level of compliance.

Important factors for the successful assessment of information security audit results are primarily:

1. Awareness and motivation of the management of critical infrastructure facilities.
2. Confidentiality.
3. Trust.

5.1. Scientific novelty. Scientific justification

The scientific uniqueness of this work lies in the proposed formalized model of information security audit for organizational compliance with international standards. The model is based on the principles of independence and objectivity of audit activities. It introduces an approach grounded in a system of objective indicators comparable to protection functions, and relies on the development of checklists with clear criteria linking indicators to verification methods. The obtained scientific result expands the scope of technical sciences in the field of cybersecurity.

5.2. Practical use

The proposed scientific solution is ready for practical implementation by audit committees, provided that auditors are adequately trained and supported by organizational management and security administrators.

5.3. Prospects for further research and study

Future research should focus on refining the methodology for developing checklists applicable to any standard or regulatory document that may require compliance audits.

Declaration on Generative AI

During the preparation of this work, the authors used ChatGPT in order to: Grammar and spelling check. After using these tools/services, the authors reviewed and edited the content as needed and take full responsibility for the publication's content.

References

[1] A. G. Petrenko, Action plan for the implementation of defense reform in 2016–2020 (roadmap for defense reform), Kyiv, DVPSP and MS of the Ministry of Defense of Ukraine, 2016.

[2] Law of Ukraine "On basic principles of ensuring cybersecurity of Ukraine", 2017. URL: https://zakon.rada.gov.ua/laws/show/2163-19.

[3] On the decision of the National Security and Defense Council of Ukraine of January 27, 2016 "On the cybersecurity strategy of Ukraine", Presidential Decree No. 96/2016, 2016. URL: https://zakon5.rada.gov.ua/laws/show/96/2016.

[4] Decision of the National Security and Defense Council of Ukraine of 10.07.17 "On the status of implementation of the decision of the NSDC of 29.12.2016 'On threats to state cybersecurity and urgent measures to neutralize them'", Presidential Decree No. 254/2017, 2017. URL: https://zakon.rada.gov.ua/laws/show/n0006525-17.

[5] Resolution of the Cabinet of Ministers of Ukraine No. 518 of 19.06.19 "On approval of general requirements for cyber protection of critical infrastructure facilities", 2019. URL: https://zakon.rada.gov.ua/laws/show/518-2019-п.

[6] Ya. V. Roi, N. P. Mazur, P. M. Skladannyi, Information security audit – the basis for effective enterprise protection, Cybersecurity: Education, Science, Technology 1 (1) (2018) 86–93. doi:10.28925/2663-4023.2018.1.8693.

[7] A. Sirotskiy, Metric approach to assessing information security in banking organizations, Sistemy bezopasnosti 25 (2016) 126–129.

[8] I. M. Kozubtsov, L. M. Kozubtsova, V. V. Kutsaiev, T. P. Tereshchenko, Methodology for assessing the cybersecurity of an organization's communication system, Modern Information Technologies in Security and Defense 1 (31) (2018) 43–46. URL: https://sit.nuou.org.ua/article/view/158236/158380.

[9] I. M. Kozubtsov, L. M. Kozubtsova, Setting the task of developing a methodology for assessing the cybersecurity of information and telecommunications systems, in: Proceedings of the International Scientific and Practical Conference "Joint Actions of Military Formations and Law Enforcement Agencies of the State: Problems and Prospects", Military Academy, Odessa Ukraine, 2019, pp. 228–229.

[10] L. M. Kozubtsova, O. I. Beskrovnyi, I. M. Kozubtsov, Structure of the methodology for evaluating the effectiveness of measures aimed at ensuring the cybersecurity of critical information infrastructure facilities, in: Proceedings of the International Scientific and Technical Conference Systems and Technologies of Communication, Informatization, and Cybersecurity: Current Issues and Development Trends, VITI, Kyiv Ukraine, 2021, p. 160.

[11] L. M. Kozubtsova, Yu. I. Khlaponyn, I. M. Kozubtsov, Methodology for assessing the effectiveness of cybersecurity measures for critical information infrastructure facilities of organizations, Modern Information Technologies in Security and Defense 2 (41) (2021) 17–22. doi:10.33099/2311-7249/2021-41-2-17-22.

[12] M. V. Artemchuk, R. M. Shtonda, I. H. Neshcheret, T. P. Tereshchenko, I. V. Tsymbal, V. O. Prydatchenko, Methodology for conducting an independent audit of an institution's information security regarding the effectiveness of information protection, Bulletin of VITI. Communication and Information Systems 2 (2021) 4–17.

[13] I. Kozubtsov, N. Lishchyna, L. Kozubtsova, I. Trush, A. Yashchuk, Information technology of information security audit of objects of critical infrastructure, in: Proceedings of the Selected Papers of the Workshop on Emerging Technology Trends on the Smart Industry and the Internet of Things, TTSIIT '2022, CEUR Workshop Proceedings, Aachen, Germany, pp. 97–106.

[14] Yu. Yakymenko, D. Rabchun, T. Muzhanova, M. Zaporozhchenko, Yu. Shchavinskyi, Technical audit of the security of information and telecommunications systems of enterprises, Cybersecurity: Education, Science, Technology 4 (20) (2023) 45–61. doi:10.28925/2663-4023.2023.20.4561.

[15] A. Desyatko, V. Gamaliy, R. Shirshov, Information technologies and systems for organizing internal auditing of enterprises, Cybersecurity: Education, Science, Technology 1 (29) (2025) 867–876. doi:10.28925/2663-4023.2025.29.947.

[16] N. Anjum, M. R. Chowdhury, Revolutionizing cybersecurity audit through artificial intelligence automation: A comprehensive exploration, Int. J. Adv. Research in Computer and Communication Engineering 13 (5) (2024) 493–502. doi:10.17148/IJARCCE.2024.13575.

[17] V. Obodyak, M. Otroshchenko, V. Lyubchak, Artificial intelligence capabilities for cybersecurity audit and risk management, Cybersecurity: Education, Science, Technology 1 (29) (2025) 319–330. doi:10.28925/2663-4023.2025.29.872.

[18] P. Lakarasu, AI for cybersecurity audits: Enhancing transparency and accountability, 2025. URL: https://medium.com/@phanishlakarasu/ai-for-cybersecurity-audits-enhancing-transparency-and-accountability-a4572a59b436.

[19] H. A. Reijers, Business process management: The evolution of a discipline, Computers in Industry 126 (2021). doi:10.1016/j.compind.2021.103404,

[20] S. I. Makarenko, Information security audit: Milestones, conceptual framework, classification of activities, Sistemy upravleniya, svyazi i bezopasnosti 1 (2018) 1–29.

[21] ISO/IEC TS 33030:2017, Information technology – Process assessment – An exemplar documented assessment process, 2017. URL: https://www.iso.org/standard/55121.html.

[22] ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection – Information security management systems – Requirements, 2022. URL: https://www.iso.org/standard/27001.

[23] H. Taherdoost, Understanding cybersecurity frameworks and information security standards: A review and comprehensive overview (2022). doi:10.3390/electronics11142181.
[24] O. Kryvoruchko, D. Gnatchenko, Functional features of the intellectual internal audit system, Cybersecurity: Education, Science, Technology 4 (24) (2024) 40–49. doi:10.28925/2663-4023.2024.24.4049.
[25] ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection – Information security controls, 2022. URL: https://www.iso.org/standard/75652.html.
[26] V. Dudikevich, O. Garasymchuk, A. Partika, Ya. Sovin, O. Nemkova, Research on the advantages of applying the method of cross-implementation of cybersecurity audit standards to counter cybercrimes using ransomware viruses, Cybersecurity: Education, Science, Technology 2 (22) (2023) 226–237. doi:10.28925/2663-4023.2023.22.226237.
[27] ISO/IEC 17799:2005, Information technology – Security techniques – Code of practice for information security management, 2005. URL: https://www.iso.org/standard/39612.html.