Management (Montevideo). 2025; 3:250
doi: 10.62486/agma2025250
ISSN: 3046-4048

ORIGINAL

Organizational Context of Security Management: Implications for Information

Contexto organizativo de la gestión de la seguridad: Implicaciones para los sistemas

Anatolii Benzar[1], Yuliia Kovalenko[2], Artem Taranenko[3], Olha Balynska[4], Igor Balynskyi[5]

[1]The Zakhidnodonbaskyi Institute of the Private Joint-Stock Company "Higher Education Institution, Interregional Academy of Personnel Management", Department of Economics and Management. Pavlohrad, Ukraine.
[2]State Non-Commercial Company "State University Kyiv Aviation Institute", Faculty of Computer Sciences and Technologies, Department of Cyber Security. Kyiv, Ukraine.
[3]The Institute of Security, Private Joint-Stock Company "Higher Educational Institution, Interregional Academy of Personnel Management". Kyiv, Ukraine.
[4]Lviv State University of Internal Affairs, Research Laboratory for the Study of Problems of Combatting Human Trafficking. Lviv, Ukraine.
[5]King Danylo University, Department of Journalism, Advertising and Public Relations. Ivano-Frankivsk, Ukraine.

Cite as: Benzar A, Kovalenko Y, Taranenko A, Balynska O, Balynskyi I. Organizational Context of Security Management: Implications for Information Systems. Management (Montevideo). 2025; 3:250. https://doi.org/10.62486/agma2025250

Submitted: 11-06-2024 **Revised:** 02-01-2025 **Accepted:** 01-06-2025 **Published:** 02-06-2025

Editor: Ing. Misael Ron

Corresponding author: Anatolii Benzar

ABSTRACT

Introduction: in the context of an unprecedented intensification and structural complication of cyber threats, which increasingly manifest as full-scale attacks on organizational entities across diverse economic clusters, the exigency of formulating and implementing conceptually sound and technologically advanced paradigms of information security management has become irrefutable.
Objective: the principal objective of this scholarly inquiry is the identification and systematic structuring of prevailing trends, as well as the analytical explication of the discursive features characterizing the implementation of innovative approaches to information security within the corporate domain.
Method: the methodological framework is grounded in a descriptive-analytical model, incorporating elements of methodological pluralism—particularly the confluence of deductive theoretical analysis of security governance paradigms and empirical reflection on secondary data pertinent to the state and specificities of such implementation.
Results: the findings substantiate the premise that the persistent escalation in the complexity of cyber threats precipitates substantial reputational, economic, and operational risks, thereby compelling organizations to recalibrate their strategic posture towards integrative models of information security governance. The most adaptive to the volatile threat landscape are risk-based and holistic approaches. Moreover, regulatory transformations within the European legal framework concerning personal data protection function as a significant catalyst in the strategic reconfiguration of information security imperatives.
Conclusions: the practical significance of this study lies in the critical generalization and systematization of the tendencies that shape the emerging epistemology of information security management in contemporary organizational structures.

Keywords: Information; Information Law; Communication; Human Rights; Information Security; Restriction of the Right to Disseminate Information.

RESUMEN

Introducción: en el contexto de una intensificación y complicación estructural sin precedentes de las

© 2025; Los autores. Este es un artículo en acceso abierto, distribuido bajo los términos de una licencia Creative Commons (https://creativecommons.org/licenses/by/4.0) que permite el uso, distribución y reproducción en cualquier medio siempre que la obra original sea correctamente citada

ciberamenazas, que se manifiestan cada vez más como ataques a gran escala contra entidades organizativas de diversas agrupaciones económicas, la exigencia de formular y aplicar paradigmas conceptualmente sólidos y tecnológicamente avanzados de gestión de la seguridad de la información se ha vuelto irrefutable.
Objetivo: el objetivo principal de esta investigación académica es la identificación y estructuración sistemática de las tendencias predominantes, así como la explicación analítica de los rasgos discursivos que caracterizan la aplicación de enfoques innovadores de la seguridad de la información en el ámbito empresarial.
Método: el marco metodológico se basa en un modelo descriptivo-analítico, que incorpora elementos de pluralismo metodológico, en particular la confluencia del análisis teórico deductivo de los paradigmas de gobernanza de la seguridad y la reflexión empírica sobre datos secundarios pertinentes para el estado y las especificidades de dicha aplicación.
Resultados: los resultados corroboran la premisa de que la persistente escalada en la complejidad y el volumen de las ciberamenazas precipita riesgos sustanciales para la reputación, la economía y las operaciones, obligando así a las organizaciones a recalibrar su postura estratégica hacia modelos integradores de gobernanza de la seguridad de la información. Los enfoques más adaptables al volátil panorama de amenazas son los basados en el riesgo y holísticos. Además, las transformaciones normativas en el marco jurídico europeo relativo a la protección de datos personales funcionan como un catalizador importante en la reconfiguración estratégica de los imperativos de la seguridad de la información.
Conclusiones: la importancia práctica de este estudio radica en la generalización y sistematización críticas de las tendencias que conforman la epistemología emergente de la gestión de la seguridad de la información en las estructuras organizativas contemporáneas.

Palabras clave: Información; Derecho a la Información; Comunicación; Derechos Humanos; Seguridad de la Información; Restricción del Derecho a Difundir Información.

INTRODUCTION

The intensive implementation of digital technologies within the managerial architecture of contemporary organizations is catalyzing the emergence of new paradigms of economic activity. These paradigms are characterized by a high degree of integration of information flows, multidimensional dependence on computational systems, and contextually determined complexity in decision-making processes. While such transformational dynamics open up new horizons for strategic flexibility and innovative self-development, they simultaneously induce an escalation of risk-prone vectors associated with information security incidents – whose complexity and variability exhibit increasingly nonlinear behavior.[1]

This phenomenon cannot be adequately understood solely through a technocratic or engineering lens; rather, it should be interpreted as an interdisciplinary construct that integrates epistemological, legal, ethical, and managerial-strategic dimensions. Information security thus becomes a critical component of organizational ontology, wherein every act of communication or data processing is a priori associated with potential vulnerabilities. Consequently, there is a growing need for unified yet adaptive mechanisms of analytical forecasting, risk compartmentalization, and reflexive management.[2] In the context of increasing cybernetic entropy, institutions operate in a post-industrial environment where risks take on a polymorphic nature, encompassing not only operational threats but also latent reputational, legal, and financial-fiscal risks. As observed by Jerman-Blažič and Bojanc,[3] based on critical-empirical analysis, organizations are compelled to increasingly invest in cyber resilience systems. These systems require not only substantial financial resources but also a paradigmatic rethinking of the very concept of security under conditions of digitalized interdependence. The economic sustainability of such investments is further reinforced by the necessity of continuous implementation of regulatory updates aligned with the evolving threat landscape.[4]

In the context of organizational information systems (IS), destructive economic consequences may arise not only from endogenous dysfunctions but also from exogenous interventions. Among the latter, information security breaches represent particularly significant incidents. One illustrative example occurred in 2017, when one of the leading U.S. credit rating agencies, following a massive data breach involving personally identifiable information, was required to pay over USD 1 billion in restitution to approximately 150 million affected individuals. In a broader historical-analytical perspective, from 2004 to 2023, the U.S. financial sector experienced over 20000 cyber incidents, resulting in cumulative material damages estimated by reputable international institutions, including the International Monetary Fund, at an astronomical USD 12 billion.[5]

Amid the rapid digitization of socio-economic processes and the escalation of cyber risks, there has been a systematic intensification of incidents involving violations of the confidentiality of personal data of information

interaction subjects. According to empirical data collected during the relevant twelve-month period of 2024, more than 70 % of business entities incorporated under the jurisdiction of the United Kingdom were subjected to fiscal sanctions amounting to or exceeding GBP 100000 for non-compliance with regulatory requirements in the area of personal data protection.[6]

Simultaneously, analytical evidence indicates that 79 % of business entities within the UK economy became victims of information security incidents aimed at undermining infrastructural integrity through the deployment of high-tech disinformation tools – particularly so-called deepfake technologies – implemented via interaction channels with external agents such as third-party suppliers and subcontractors. This figure represents a more than 20 % increase compared to 2023,[6] pointing to the stagnation of institutional response mechanisms.

On a global scale, the situation appears even more alarming. According to the U.S.-based Identity Theft Resource Center, over one billion data compromise incidents were identified during just the first half of 2024 – a 490 % increase compared to the corresponding period of the previous year.[7] This inflation of digital threats underscores not only the evolution of attack methodologies but also the insufficient adaptation of defensive protocols within the corporate environment.

An expert survey conducted in May 2024 by the consulting firm KPMG among 200 companies revealed that 40 % of respondents – senior executives responsible for cybersecurity – confirmed that their organizations had experienced attacks. Furthermore, 76 % expressed significant concern regarding the increasing complexity and polymorphism of emerging cyber threats,[8] whose sources include both highly professional transnational cybercriminal conglomerates and internal actors, such as employees or affiliated contractors.

Accordingly, the multidimensionality of threats in the realm of information security is evident – not only through data leakage phenomena but also via scalable attacks and cyber fraud carried out through modern communication platforms. This reality necessitates an urgent reevaluation of foundational paradigms and the development of adaptive, multidisciplinary strategies for managing information security within corporate structures.

The purpose of this article is to undertake a comprehensive examination of the prevailing trajectories in the evolution and distinctive features of the implementation of innovative paradigms of information security management within corporate environments, through the lens of a syncretic analysis of transdisciplinary approaches that integrate both regulatory-legal and techno-organizational dimensions of countering cyber threats amid the escalating complexity of digital infrastructures and the dynamic nature of globalized risks.

Literature review

Within the paradigmatic framework of post-nonclassical interpretations of digital reality, the construct of information security emerges as a transversal phenomenon rooted in the discursive field of strategic cognitivism. Its ontological essence is expressed through the tripartite lens of integrity, availability, and confidentiality of informational substrata, axiomatically oriented toward the poly-subjective interests of institutionalized stakeholders.[9]

Contemporary academic literature, engaging in an eclectic deconstruction of the subject matter, delineates a multiplicity of approaches to information security governance, each constituting a distinct theoretical-practical corpus with its own epistemological grounding.[10] Eloff and von Solms[11] derive their managerial methodology from the invariants of international regulatory frameworks, constructing a unified classificatory schema of security protocols that tends toward quasi-systemic representations of infrastructural resilience.

In contraposition to this stance, Lee[12] articulates a synthetic model of cyber-risk governance wherein technospheric engineering is interlaced with psychosocial modalities, thereby engendering a heterogeneous structure of risk management characterized by holistic synthesis. A congruent epistemological posture is evident in the work of Soomro et al.,[2] who employing categories of applied hermeneutics, identify six fundamental vectors that constitutively determine the efficacy of information security governance: policy formalization, cognitive elevation of personnel, architectural transformation of IT environments, emergent alignment of business and technological processes, cybernetic management of human capital, and hierarchical coordination of informational-resource frameworks.[13,14]

Within the logic of normative pluralism, Eloff and Eloff[15] propose a multi-component security model, determined by the internalization of policies, standardized conventions, deontological codes of conduct, technical guidelines, legal axioms, and ethical imperatives – elements which, in their totality, engender a quasi-organic cybersecurity system.

Kaushik[16] advances an intellectually rigorous approximation to a comprehensive cybersecurity paradigm, substantiating the relevance of an adaptively inductive architecture wherein blockchain protocols and machine learning algorithms serve as vectors of paradigmatic transformation. Empirical validation of this doctrine within small and medium-sized enterprises on the Iberian Peninsula demonstrates enhanced operational resilience through the implementation of ISO-27001:2013 and the institutionalization of audit procedures, workforce requalification, and certification validation mechanisms.[17]

Conversely, Stewart and Jürjens[1] advocate for a hermeneutically flexible approach characterized by modular recalibration of managerial practices in accordance with corporate identity. Nevertheless, such an approach necessitates constant emergent calibration of compliance processes, dynamic remediation of regulatory lacunae, and the continuous monitoring of procedural integration.

From the perspective of security protectionism, preventive and coercive-control paradigms, albeit marginal in mainstream discourses, are occasionally referenced as relevant under conditions of extreme risk exposure.[18,19]

Fenz et al.[20] define risk management through a systematic lens, encompassing asset inventory, threat modeling, resource valuation, probabilistic risk forecasting, interorganizational knowledge exchange, and alignment of anticipated losses with protective investments. The conceptual model of Jerman-Blažič and Bojanc[3] introduces high-level risk modeling for optimizing investment in defensive infrastructure, grounded in budgetary rationalization and enabling the suboptimal allocation of resources.

In a similar vein, Meszaros and Buchalcevova[21] propose a technically sharpened approach to security management through threat and risk approximation, emphasizing financial efficiency. Within such dichotomies between asset valuation and resource constraints, the findings of Weishäupl et al.[4] underscore the strategic merit of selective investment methodologies.

Alahmari and Duncan[22] underscore the influence of sociobehavioral determinants – including employee behavior, awareness levels, and managerial decision-making structures – on the efficacy of cyber-risk governance in SMEs. In a critical vein, Ganin et al.[23] caution against reducing governance to purely risk-regulative models, arguing that such reductionism, despite its structural appeal, fails to capture the full ontological scope of organizational management.

Recent scholarly contributions emphasize the growing complexity of managing organizational information security in the era of digital transformation and global informatization. Bondarenko et al.[24] stress the need for integrating strategic planning within national security frameworks to better address informational threats. Similarly, the legal dimension of cybersecurity is explored by Bondarenko et al.,[25] highlighting the significance of robust regulatory mechanisms in digital environments. Broader societal and infrastructural implications are discussed by Chmyr et al.[26] and Hren et al.[27] who examine how the global information space and societal perceptions of information security influence national and organizational resilience. Lelyk et al.[28] provide an applied perspective, analyzing enterprise-level economic security through integrated information protection measures. Finally, Likarchuk[29] extends the discussion into the geopolitical realm, emphasizing how global identity and international cooperation shape the contours of state and organizational information security strategies.

In summation, the holistic approach to information security governance demonstrates conceptual superiority over fragmented models, as it ensures integrative coverage of both material-technological and normative-ethical, cognitive-behavioral, and administrative dimensions, ultimately producing a metastable system of cyber-resilience capable of adaptive performance within conditions of high informational turbulence.

METHOD

The research was conducted within a descriptive-analytical methodological framework, designed to provide a multifaceted examination of contemporary concepts and empirical determinants associated with the application of various approaches to information security management in organizational structures. The methodological eclecticism of the study, based on a synthesis of qualitative and quantitative procedures, justified the implementation of a two-stage heuristic strategy that ensured the depth, representativeness, and relevance of the findings. At the initial stage, a targeted content analysis of a relevant corpus of scholarly publications was carried out, wherein the conceptual category of "information security management approaches" is operationalized and its foundational components are deconstructed. As a result, the most frequently articulated management paradigms in academic discourse – namely, the holistic, flexible, and risk-oriented approaches – were identified and typologized in terms of their respective advantages and structural-functional limitations. The content analysis of scientific publications covered the period from 2010 to 2024. The sample of scientific publications was formed according to the semantic field of the study, using the Google Scholar database with the following keywords: information, information security, confidentiality, information infrastructure, cyber threats, cyber risks, data protection, digital infrastructure, security policies, incident management. The criteria for including scientific publications in the study included: 1) empirical validity of the research results; 2) a systematic approach to the analysis of information security risks and organizations' approaches to cyber threat management; 3) coverage of the organizational level of information security management; 4) the presence of a critical analysis of the implementation of international information security management standards; 5) coverage of the global and regional context of information security management practices; 6) peer-reviewed journals indexed in Scopus/Web of Science.

The second stage of the research involved the extrapolation and systematic analysis of secondary empirical

data sources that reflect the practical implementation of the aforementioned approaches in the activities of corporate and institutional entities. Specifically, the following sources were employed: Hiscox Cyber Readiness Report[30] – for identifying levels of cyber readiness among companies in a transnational context; Statista[31] – a global survey of Chief Information Security Officers (CISOs), which enabled the identification of the most threatening and probable cyber risks; Corporate representatives' survey by Gartner[32] – providing insights into the actual state of information security management across various sectors; KPMG[8] – targeted findings from a May 2024 survey of 200 CISOs, focused on emerging threats and defensive strategies; ISMS Survey[33] – analytical data regarding the extent of implementation of the international ISO/IEC 27001 standard in the corporate domain. Secondary data mainly covers the global context in the field of information security, focusing on large companies in the corporate sector. At the same time, the sample includes the financial, technology, telecommunications, energy, manufacturing, industrial, pharmaceutical, government, healthcare, and small and medium-sized business sectors (Table 1). To eliminate bias in KPMG's sample selected for the analysis of secondary sources of information, the survey results were interpreted taking into account the limited number of respondents, mainly multinational corporations in developed countries.

The integrated application of a polymethodological approach enabled a high degree of validity in representing current trends, exogenous factors, and institutional determinants of information security management practices, with particular emphasis on comparing the effectiveness of holistic and risk-oriented managerial models within a dynamically evolving operational environment.

Table 1. Characteristics of secondary data for the study of practical implementation of information security approaches in organizations

Source	Data type	Geographical coverage	Sectoral coverage
Hiscox Cyber Readiness Report	Report on the cyber readiness levels of companies, 2024 (2,150 respondents in the field of information security management, survey conducted in August–September 2024)	Global context	Small and medium-sized businesses, large corporations, with an emphasis on the financial and technology sectors. The sample included the following sectors: trade, healthcare, construction, manufacturing, telecommunications, business services, and others.
Statista	CISOs survey on different types of threats, January–February 2024 (1,600 respondents)	Global context	Corporate sector with a focus on companies with critical digital infrastructure
Corporate representatives' survey by Gartner	Analysis of the state of information security management and the most common types of threats for 2020-2023	Regional and global dimension with a focus on Europe and the US	Financial sector, healthcare, industry, IT, public sector
KPMG	CISOs survey on new types of cyber threats and defense strategies for 2024 (227 information security executives)	The US and international markets	Transnational corporations, including the banking sector, telecommunications, pharmaceuticals, and energy sectors
ISMS Survey	Data on the level of implementation of ISO/IEC 27001 in the corporate sector	Europe, global context	The corporate sector, mainly IT companies, covering manufacturing, telecommunications, and transportation industries

RESULTS AND DISCUSSION

The contemporary architecture of information security governance within organizational structures is undergoing increasingly intensive transformation under the influence of a multitude of exogenous determinants, primarily regulatory shifts, technosocial disruptions, and normative-value deviations, which collectively give rise to a new epistemology of the security discourse. Within this context, the imperative consideration lies in the radical transformation of the legal framework, prompted, inter alia, by the alarming expansion in the volume of personally identifiable data, the transjurisdictional nature of its circulation, and the objectified necessity of formalizing privacy protection mechanisms as a fundamental attribute of digital subjectivity.[34] In this regard, Stoll's[9] assertion remains particularly pertinent: the intensification of legal imperatives, coupled with recurrent data breaches, has significantly amplified the need to safeguard data confidentiality.

The substantive reconfiguration of legal institutions is primarily directed at eliminating the jurisdictional atomization prevalent in the implementation of data protection norms, while simultaneously mitigating axiological and procedural ambiguity surrounding the interpretation of security within the digitized interaction

between individuals and information systems. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 operates as a codified embodiment of institutional accountability on the part of data controllers and processors, mandating the adaptive implementation of comprehensive security measures commensurate with the gradation of risks associated with the processing of sensitive data.[35]

A paradigmatic milestone in the legal codification of information security was the adoption of the first pan-European regulatory framework – the Directive on Security of Network and Information Systems – which, de facto, articulates the obligatory implementation of risk-oriented protocols by digital entities responsible for the operation of critical infrastructure. These entities include enterprises that underpin the functionality of essential socio-economic systems and, consequently, constitute high-value targets of sophisticated cyber threats.[36] The Directive imposes an obligation upon EU Member States to develop national cybersecurity strategies incorporating clearly delineated institutional roles within the framework of public–private collaboration.[37]

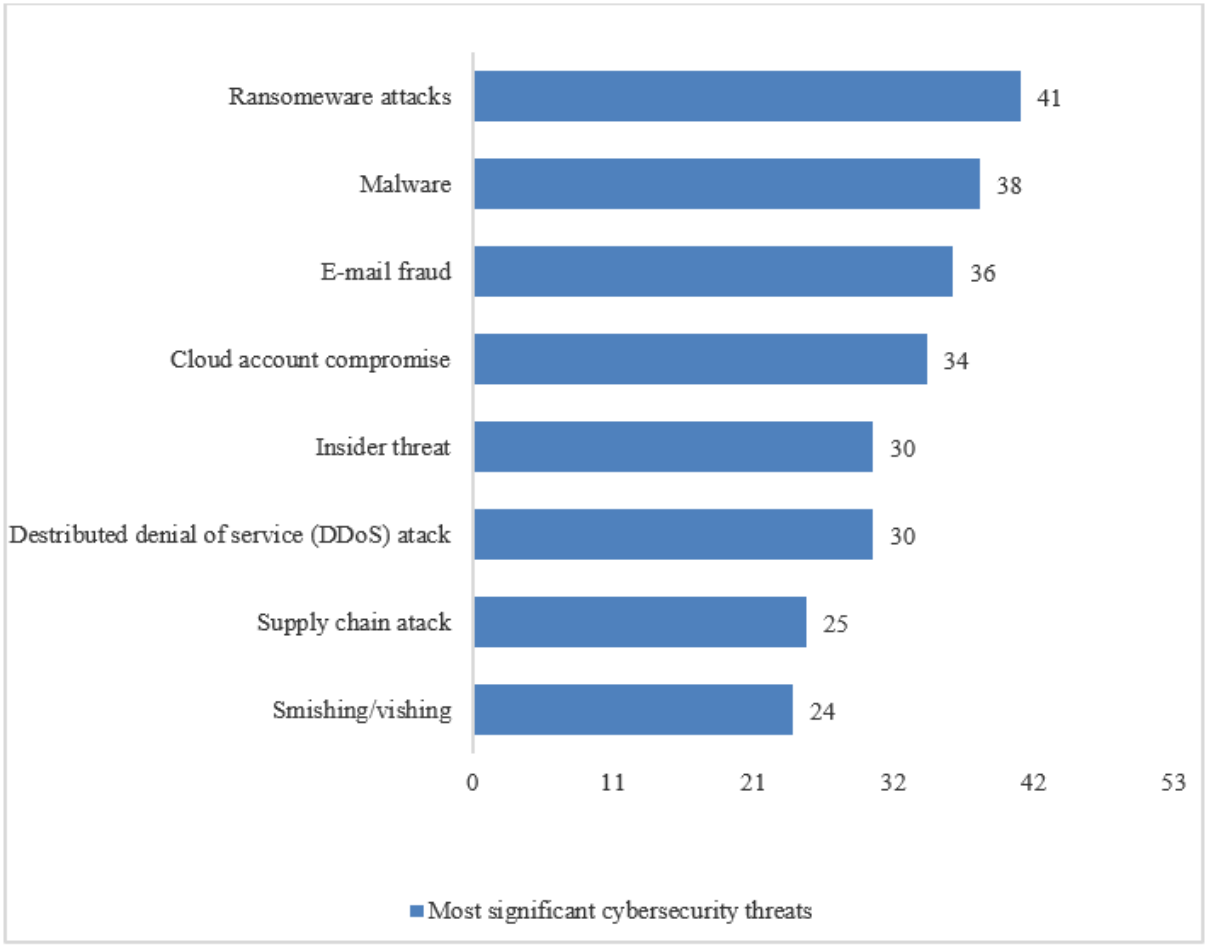
An additional instrument of institutional legitimization in the realm of cybersecurity is the certification infrastructure established by the EU Cybersecurity Act, which lays the foundation for a trans-European mechanism of accreditation for technologies, services, and processes. The amendments adopted in April 2023 to the aforementioned Act marked a transition toward the systematic development of certification schemes for managed security services, including incident response, testing, security auditing, and consulting practices.[38] These innovations are teleologically oriented toward the unification of quality standards in the field of information protection.

Such regulatory developments are wholly justified in light of the ever-increasing technological dependence on extraterritorial IT service providers, particularly within the financial sector. Given the proliferating role of artificial intelligence in configuring information security protocols, the utilization of managed services – characterized by a high level of specialization – continues to expand, significantly enhancing organizational cyber-resilience in the face of increasingly complex threats. An empirically relevant case was the ransomware attack of 2023, during which vulnerabilities in cloud providers paralyzed the operations of 60 credit unions in the United States.[5] Equally symptomatic is the escalating complexity and polymorphic nature of information threats, which are progressively evolving in scope and intensity. According to the Hiscox Cyber Readiness Report,[30] the period from 2020 to 2024 witnessed a 36 % increase in cyberattacks targeting small enterprises – a sector traditionally deemed less protected yet strategically vulnerable. In response, average corporate expenditure on cybersecurity rose by 39 % between 2020 and 2023, underscoring the crystallization of security as a strategic priority rather than merely a technical necessity.

Data from the Global Chief Information Security Officer Organization and Compensation Survey[39] further indicates that 41 % of respondents identified ransomware attacks as the most severe threat vector, followed by malicious software (38 %) and email-based fraud (36 %), collectively constituting a multidimensional topography of contemporary cyber risk (figure 1).

Tent escalation of cybernetic threats – both exogenous and endogenous in nature – contemporary business entities increasingly find themselves immersed in a paradigmatically novel architecture of risks that directly jeopardize the resilience of their informational infrastructure. Among the multitude of destabilizing factors contributing to the fragmentation of security systems, particular emphasis must be placed on the chronic shortage of qualified human capital, the methodological obsolescence of managerial practices, and the irreversible complication of cyber threat vectors, which frequently transcend conventional risk taxonomies. Compounding this situation is the insufficient cognitive engagement of personnel with respect to the systemic importance of information security. This exigency necessitates the institutionalization of comprehensive information security policies at the intra-organizational level, with strict adherence to prescribed protocols as an instrument for reshaping behavioral patterns towards compliance and the internalization of digital ethics.[40] An imperative condition for elevating the degree of security-related awareness within the organizational structure is the relational exchange of knowledge, which functions as a catalyst for the transfer of experiential insights and ontological understanding of informational vulnerabilities.[41]

In this regard, corporate governance structures tend to implement hybridized information security schemes wherein endogenous organizational resources are synergistically combined with highly specialized exogenous expertise. In support of this trend, empirical data derived from a survey conducted in May 2024 among 200 senior information security executives underscore the prevalence of risk-oriented paradigms in contemporary security management. Specifically, 76 % of respondents confirmed a high level of awareness regarding internal vulnerabilities and zones of potential threat within their organizations,[8] indicating a maturing managerial awareness of critical digital exposure points. Furthermore, 86 % of executives reported that Security Operations Centers (SOC) are operating at a level of preparedness adequate to resist complex and structurally sophisticated attacks, while 90 % affirmed complete control over risk-prone segments of the digital infrastructure.[8] It is noteworthy that the average annual operational budget for SOCs reached USD 14.6 million, with 37 % allocated to threat prevention and anomaly detection.[8]



Source: Statista[31]

Figure 1. Subjectivized Stratification of the Most Perceptually Salient Vectors of Cyber Threats to Institutionalized Economic Entities in the Global Context, Based on the Expert Appraisal of Chief Information Security Officers as of February 2024

According to the conceptual framework proposed by Shameli-Sendi et al.,[42] one of the most effective and systemically justified approaches to the deconstruction of information risks within corporate structures is a risk-prioritized strategy. Within this paradigm, as noted by Shamala et al.,[43] a methodologically calibrated process prevails – one that encompasses the delineation of assessment zones, aggregation of relevant data, extrapolation of risk determinants, and the articulation of a security profile for critically sensitive informational assets.

The implementation of holistic security concepts has become increasingly salient, particularly through their institutionalization in international regulatory instruments – most notably the ISO/IEC 27001 standard. This standard integrates elements of information security, cybersecurity, and privacy into a unified framework of procedural compliance. It enables organizations to construct comprehensive Information Security Management Systems (ISMS) by applying risk-adaptive methodologies tailored to the size, operational complexity, and strategic profile of the entity.[44]

The formation of an ISMS is intrinsically linked to the organization's strategic goals, internal processes, hierarchical configuration, corporate culture, and governance model. Hence, ISO/IEC 27001 transcends its role as a mere regulatory document, evolving instead into a principal vector of strategic cyber governance. In this context, Stoll[9] reports that over 1,5 million organizations worldwide have adopted standardized ISMS frameworks, with the highest concentration found within the high-technology sector, where certification serves not only as an indicator of security maturity but also as a lever for competitive advantage.[45]

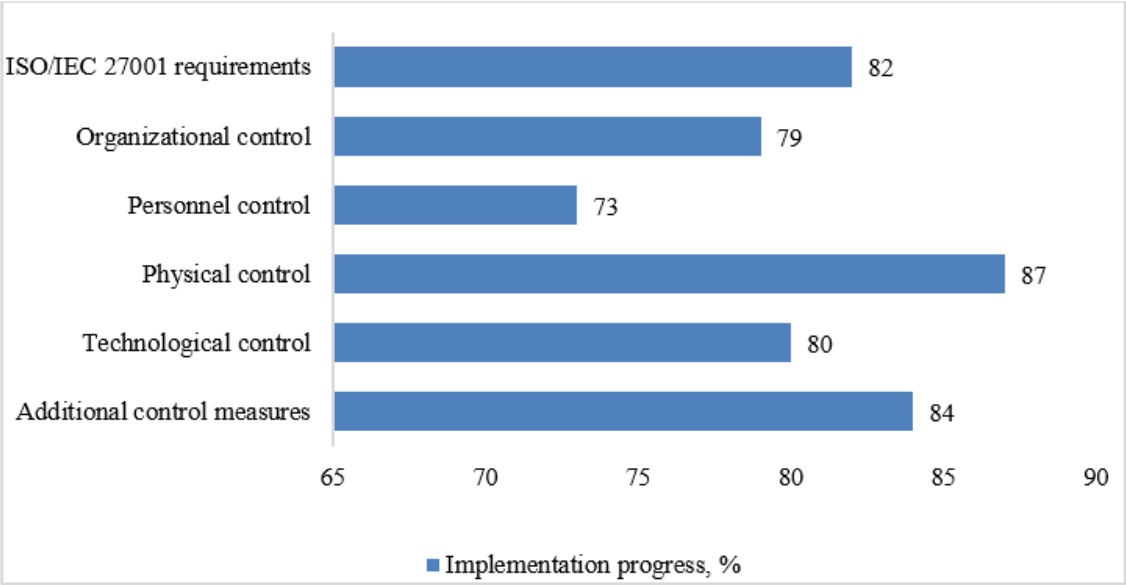
The geopolitical dimension of the standard's proliferation must also be acknowledged. In several national jurisdictions, such as the Republic of Moldova, the implementation of ISO/IEC 27001 has acquired official legitimacy within the framework of state cybersecurity strategies. Notably, the Information Security Strategy of the Republic of Moldova for 2019–2024 mandates organizational compliance with international standards, including ISO/IEC 27001, as a means of safeguarding digital assets and fostering trust among foreign investors.[46]

Undoubtedly, the discursive comprehension of the effectiveness of ISO/IEC 27001 implementation in the domain of information security necessitates not only empirical reflection but also profound epistemological

analysis regarding the institutional legitimacy of this approach within diverse socio-technical contexts. As Kamil et al.[47] aptly observe, a paradoxical dichotomy emerges between the normative universality of the aforementioned standard and the actual level of competence demonstrated by its implementers, given that the cognitive capacity of implementation agents directly correlates with the standard's operational efficacy. Consequently, within the Swedish corporate environment, a pronounced dispersion can be observed in the degree of normative integration of ISO/IEC 27001 – ranging from full institutionalized compliance to merely nominal implementation lacking substantive depth.

Simultaneously, according to the analytical insights of Culot et al.,[48] the very process of institutional adoption of ISO/IEC 27001 exhibits a tendency toward fragmentation, stemming from a misalignment between its theoretical-normative foundations and the practical vectors of implementation. The authors underscore the limited availability of empirical evidence convincingly attesting to the effectiveness of the standard as a unified instrument for ensuring information security, particularly in the context of the transnational digital ecosystem, wherein regulatory efficacy tends to manifest situationally.

At present, the process of automating ISO/IEC 27001 compliance requirements has reached a quantitative threshold in 82 % of cases (figure 2), signifying a gradual shift from manual administration to algorithmically governed control models. Specifically, software suites designed to support the standard ensure organizational-level control at a rate of 79 %, indicating a systemic unification of managerial practices. Control over human resources (73 %) and physical parameters (87 %) points to an intensifying material and anthropocentric synergy within security mechanisms, while the technological dimension (80 %) confirms the high adaptability of infrastructural architectures to information protocol requirements. Finally, the implementation of supplementary control measures, recorded at 84 %, demonstrates a trend toward extrapolating the standard beyond its foundational imperatives.



Source: ISMS[33]

Figure 2. Dynamics of the Operationalization Trajectory of ISO/IEC 27001: A Multiphase Integration Paradigm

Undeniably, within the framework of the evolutionary transformation of paradigms governing information security management in the contemporary cyber-physical landscape, the application of conceptual matrices – particularly the cybersecurity framework elaborated by the U.S. National Institute of Standards and Technology (NIST) – has acquired increasing epistemological significance. This framework, functioning as a multilayered architecture of continuous processes, embodies a heterogeneous synthesis of institutional risk management, structural control, and the dynamic resilience of organizational infrastructures.[49] Within this conceptual dichotomy, five distinct functional domains are delineated, realized through cyclical transition and mutual reinforcement: Identification – the implementation of a systemic approach to modeling cybersecurity risks, mandating the identification of critical informational assets, personnel taxonomy based on access levels, and the definition of potential vectors of vulnerability; Protection – the formalization of preventive protocols, including cryptographic mechanisms, access control policies, institutional segmentation of internal networks, and software-hardware means of ensuring integrity; Detection – the installation of systems for both retrospective and prospective monitoring, employing telemetry-based anomaly sensors and embedded indicators of compromise; Response – the codification of incident response algorithms, emphasizing the rapid

deconfiguration of compromised segments and the activation of internal analytical procedures; Recovery – the development of post-incident reparative scenarios aimed at the emergent restoration of operational capacity and the minimization of latent threat vectors.

Within the framework of post-nonclassical epistemology of information security – which is increasingly conceptualized as a polycentric and self-organizing phenomenon – the strategic management of organizational security parameters can no longer be constrained by the reductionist paradigms of the past. In an era marked by the progressive integration of digital agents into heterarchical informational ecosystems, there emerges an acute imperative to revise entrenched normative-functional models, previously predicated on linear-causal risk response schemas. Consequently, contemporary theoretical and applied approaches increasingly invoke transdisciplinary constructs that amalgamate elements of quantum logic, poststructuralist deconstruction, and cybernetic operationalism.

In light of the foregoing, the following table serves as a conceptual matrix that systematizes key strategies for managing organizational information security, as delineated through their epistemological grounding, institutional implementability, and evaluative indices. It is crucial to underscore that the paradigms herein presented do not constitute a hierarchical typology but rather reflect a plurality of concurrently operative yet methodologically incommensurable approaches, each delineating a distinct trajectory of interaction between informational vulnerability and systemic resilience. Thus, the analytical engagement with these strategems serves not merely as an instrument of managerial intervention but also as a methodological framework for subsequent intellectual extrapolations in the field of informational hermeneutics.

Table 2. Contemporary Strategies for Managing Organisational Information Security

Strategic Paradigm	Epistemological Foundations	Implementation Complexities	Evaluative Metrics
Post-Structural Cyber Governance	Rooted in Foucauldian discourses of power-knowledge interplay, this approach interrogates normative security architectures through a deconstructionist lens.	The integration of discursive cybersecurity protocols often encounters resistance from legacy frameworks entrenched in deterministic epistemes.	Effectiveness is gauged via dialectical hermeneutics applied to socio-technical incident narratives.
Quantum-Cryptographic Risk Containment	Drawing upon principles of quantum indeterminacy and Heisenbergian uncertainty, it reconceptualizes data as probabilistic rather than static entities.	Operationalization is impeded by infrastructural incompatibility and the ontological volatility of subatomic key exchanges.	Metrics include probabilistic fidelity indices and decoherence thresholds within entropic models.
Meta-Adaptive Ethical Firewalls	Grounded in post-Kantian technoethics, these systems modulate moral imperatives in real time through neuro-symbolic inference engines.	The design necessitates transdisciplinary synthesis, merging affective computing with deontological AI heuristics.	Evaluation hinges on paradox resilience and the dynamic equilibrium of normative flux.
Polycentric Threat Topologies	Informed by polyarchy theory and rhizomatic organizational models, this strategy decentralizes authority to proliferate adaptive nodes of security cognition.	Implementation challenges arise from the semiotic dissonance between hierarchical IT governance and emergent network fluidity.	Success is measured via nodal elasticity indices and resilience vectors in stochastic threat matrices.
Socio-Algorithmic Immuno-Resilience	Embeds Luhmannian systems theory with autopoietic machine learning, treating security ecosystems as self-referential yet externally modulated entities.	Complexity emerges from reconciling closed-system logic with ambient threat vectors that transgress systemic boundaries.	Metrics include systemic autopoiesis coefficients and cybernetic entropy modulation rates.

Source: compiled authors based on Bondarenko et al.,[24] Bondarenko et al.,[25] Chmyr et al.,[26] Hren et al.,[27] Lelyk et al.,[28] Likarchuk[29]

Accordingly, the systemic incorporation of such framework-based constructs into organizational strategies of information security management reflects an increasing differentiation of compliance requirements within the normative-legal domain. Particularly noteworthy are the imperatives mandating the implementation of both technical and organizational-institutional measures for mitigating cyber risks by providers and operators of digital services. Moreover, the necessity of certifying information and communication technologies in accordance

with predefined security criteria has been elevated as a manifestation of meta-institutional oversight.

Given the intensification of destructive informational vectors, corporate cyber-readiness emerges not merely as an indicator of resilience, but as a strategic determinant of organizational viability. This engenders a deeper integration of risk-oriented methodologies, which in turn accentuate the diagnosis of latent vulnerabilities and the construction of risk hierarchies. The standardized management system, embodied in ISO/IEC 27001, thus represents not merely a normative framework, but a synthetic paradigm of organizational informational resilience – one that has effectively assumed the status of a de facto dominant model within the domain of corporate cybersecurity.

Conclusions. The escalation in both the frequency and sophistication of cyber threats infiltrating the operational contours of contemporary organizations has evolved into a complex risk paradigm encompassing economic, functional, and reputational dimensions of loss. In response to this latent yet intensifying menace, corporate actors are increasingly implementing system-integrative approaches to information security management, among which the holistic and risk-based methodologies prevail.

The holistic approach inherently entails the structuring of a comprehensive architecture for managing security processes, in which each component is interlinked with the institutional and technological subsystems of the organization. In contrast – though not in contradiction – the risk-oriented approach undertakes a targeted identification of vulnerabilities, focusing on the prioritization of threats and the proportional implementation of countermeasures, which may, in turn, be incorporated within the overarching holistic paradigm.

At the macro level, information security is institutionalized not merely as a defensive function, but as a determinant in the formulation of new strategic competitive advantages, particularly within the context of global market digitalization. An additional impetus to the evolution of the regulatory culture in managing security risks has been introduced by the European Union's legislative innovations concerning the protection of personal data. These legal interventions have fundamentally reshaped the juridical topology of obligations for entities engaged in processing sensitive data, imposing requirements to implement preventive security mechanisms based on individualized risk profiles. Of particular significance is the legal imperative for transparency and mandatory reporting of security incidents, which imposes increased accountability on digital service providers.

Moreover, the expansion of institutional authority in the certification of information and communication technology products, services, and processes not only codifies standards of quality but also transforms regulatory norms into instruments for legitimizing market competitiveness.

Simultaneously, it is necessary to acknowledge a critical empirical limitation of the study: the absence of comprehensive, representative data on the practical implementation of information security management approaches at the level of individual organizations significantly restricts the ability to identify typical dysfunctions and barriers in the cyber security domain. A thorough examination of this issue in an applied dimension would facilitate the concretization of strategic challenges and the development of adaptive models for security governance.

REFERENCES

1. Stewart H, Jürjens J. Information security management and the human aspect in organisations. Information Computer Security 2017;25(5):494–534. https://doi.org/10.1108/ICS-07-2016-0054

2. Soomro ZA, Shah MH, Ahmed J. Information security management needs more holistic approach: A literature review. International journal of information management 2016;36(2):215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

3. Jerman-Blažič B, Bojanc R. An economic modelling approach to information security risk management. International Journal of Information Management 2008;28(5):413–422. https://doi.org/10.1016/j.ijinfomgt.2008.02.002

4. Weishäupl E, Yasasin E, Schryen G. Information security investments: An exploratory multiple case study on decision-making, evaluation and learning. Computers Security 2018;77:807–823. https://doi.org/10.1016/j.cose.2018.02.001

5. International Monetary Fund. Rising Cyber Threats Pose Serious Concerns for Financial Stability. [Internet]. 2024 [cited 28 May 2025]; Available in: https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability

6. Alliantist. The State of Information Security Report 2024. [Internet]. 2024 [cited 28 May 2025]; Available in: https://www.isms.online/state-of-infosec-24/

7. International Information Systems Security Certification Consortium, ISC2. ISC2 Survey: More Cybersecurity

Leadership Training Needed. [Internet]. 2024 [cited 28 May 2025]; Available in: https://www.isc2.org/insights/2024/12/isc2-survey-cybersecurity-leadership?queryID=77c010de9f13e0df2cb0b77c783e43f9

8. KPMG. KPMG Survey: C-Suite Cyber Leaders Optimistic about Defences, but Large Percentage Suffered Recent Cyber Attack. [Internet]. 2024 [cited 28 May 2025]; Available in: https://kpmg.com/us/en/media/news/2024-cybersecurity-survey.html

9. Stoll M. An information security model for implementing the new ISO 27001. In: Handbook of Research on Emerging Developments in Data Privacy. (pp. 216–238). IGI Global, 2015. https://doi.org/10.4018/978-1-4666-7381-6.ch011

10. Tvaronavičienė M, Plėta T, Della Casa S, Latvys J. Cyber security management of critical energy infrastructure in national cybersecurity strategies: Cases of USA, UK, France, Estonia and Lithuania. Insights into regional development 2020;2(4):802–813. https://doi.org/10.9770/ird.2020.2.4(6)

11. Eloff MM, von Solms SH. Information security management: A hierarchical framework for different approaches. Computers Security 2000;19(3):243–256. https://doi.org/10.1016/S0167-4048(00)88613-7

12. Lee I. Cybersecurity: Risk management framework and investment cost analysis. Business Horizons 2021;64(5):659–671. https://doi.org/10.1016/j.bushor.2021.02.022

13. Tarasenko O, Lysenko S, Tarlopov I, Pidkaminnyi I, Verhun M. Analysis of the competitiveness of higher education institutions in Ukraine in the context of recovery and development after the war. Multidisciplinary Science Journal 2024;6:e2024ss0210. https://doi.org/10.31893/multiscience.2024ss0210

14. Lysenko S, Skurativkyi R. Extended Special Linear group ESL2(F) and matrix equations in SL2(F):SL2(Z) and GL2(Fp). Wseas Transactions on Mathematics 2024;23:643–659. https://doi.org/10.37394/23206.2024.23.68

15. Eloff JH, Eloff M. Information security management: a new paradigm. In: Proceedings of the 2003 annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology. (pp. 130–136). SAICSIT. [Internet]. 2024 [cited 28 May 2025]; Available in: https://www.sis.pitt.edu/jjoshi/courses/is2621/SecManParadigm2.pdf

16. Kaushik M. Cybersecurity Management: Developing Robust Strategies for Protecting Corporate Information Systems. International Journal for Global Academic Scientific Research 2024;3(2):24–35. https://doi.org/10.55938/ijgasr.v3i2.75

17. Antunes M, Maximiano M, Gomes R, Pinto D. Information security and cybersecurity management: A case study with SMEs in Portugal. Journal of Cybersecurity and Privacy 2021;1(2):219–238. https://doi.org/10.3390/jcp1020012

18. Ahmad A, Maynard SB, Park S. Information security strategies: Towards an organisational multi-strategy perspective. Journal of Intelligent Manufacturing 2014;25:357–370. https://doi.org/10.1007/s10845-012-0683-0

19. Chen Y, Ramamurthy K, Wen KW. Organisations' information security policy compliance: A stick or carrot approach? Journal of Management Information Systems 2012;29(3):157–188. https://doi.org/10.2753/MIS0742-1222290305

20. Fenz S, Heurix J, Neubauer T, Pechstein F. Current challenges in information security risk management. Information Management Computer Security 2014;22(5):410–430. https://doi.org/10.1108/IMCS-07-2013-0053

21. Meszaros J, Buchalcevova A. Introducing OSSF: A framework for online service cybersecurity risk management. Computers Security 2017;65:300–313. https://doi.org/10.1016/j.cose.2016.12.008

22. Alahmari A, Duncan B. Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. In: 2020 international conference on cyber situational awareness, data analytics and assessment (CyberSA). (pp. 1–5). IEEE, 2020. https://doi.org/10.1109/CyberSA49311.2020.9139638

23. Ganin AA, Quach P, Panwar M, Collier ZA, Keisler JM, Marchese D, Linkov I. A multicriteria decision

framework for cybersecurity risk assessment and management. Risk Analysis 2020;40(1):183–199. https://doi.org/10.1111/risa.12891

24. Bondarenko S, Bratko A, Antonov V, Kolisnichenko R, Hubanov O, Mysyk A. Improving the state system of strategic planning of national security in the context of informatization of society. Journal of Information Technology Management 2022a;14:1–24. https://doi.org/10.22059/jitm.2022.88861

25. Bondarenko S, Makeieva O, Usachenko O, Koval S, Tkachenko T. The legal mechanisms for information security in the context of digitalization. Journal of Information Technology Management 2022b;14:25–58. http://doi.org/10.22059/JITM.2022.88868

26. Chmyr Y, Nekryach A, Kochybei L, Solodka M, Myroniuk O. Postindustrial society and global informational space as infrastructure medium and factor for actualization of the state informational security. Contributions to Political Science 2023;136:61–73. https://doi.org/10.1007/978-3-031-33724-6_4

27. Hren L, Karpeko N, Kopanchuk O, Dzyuba S, Polishchuk I. Substantive essence and components of the societal phenomenon "Information Security" in the age of information society. Contributions to Political Science 2023;136:75–91. https://doi.org/10.1007/978-3-031-33724-6_5

28. Lelyk L, Olikhovskyi V, Mahas N, Olikhovska M. An integrated analysis of enterprise economy security. Decision Science Letters 2022;11(3):299–310. https://doi.org/10.5267/j.dsl.2022.2.003

29. Likarchuk N. Information state in the context of international security and global identity: Challenges and prospects. International Relations: Theory and Practical Aspects 2024;14:107–121. https://doi.org/10.31866/2616-745X.14.2024.319359

30. Hiscox Cyber Readiness Report. [Internet]. 2024 [cited 28 May 2025]; Available in: https://www.hiscoxgroup.com/cyber-readiness

31. Statista. The most significant cybersecurity threats in organisations worldwide according to Chief Information Security Officers (CISOs) as of February 2024. [Internet]. 2024 [cited 28 May 2025]; Available in: https://www.statista.com/statistics/1350460/cybersecurity-threats-at-companies-worldwide-cisos/

32. Gartner Survey Reveals Only 14 % of Security Leaders Successfully Balance Data Security and Business Objectives. Gartner. [Internet]. 2025 February 11 [cited 28 May 2025]; Available in: https://www.gartner.com/en/newsroom/press-releases/2025-02-11-gartner-survey-reveals-only-14-percent-of-security-leaders-successfully-balance-data-security-and-business-objectives

33. ISMS. The proven path to ISO 27001 success. [Internet]. 2024 [cited 28 May 2025]; Available in: https://www.isms.online/solutions/achieve-iso-27001/

34. Official Journal of the European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). [Internet]. 2024a [cited 28 May 2025]; Available in: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX %3A32016R0679

35. European Council. The general data protection regulation. [Internet]. 2024 [cited 28 May 2025]; Available in: https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation/

36. Official Journal of the European Union. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). [Internet]. 2024b [cited 28 May 2025]; Available in: https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng

37. European Commission. Directive on Security of Network and Information Systems. [Internet]. 2024a [cited 28 May 2025]; Available in: https://ec.europa.eu/commission/presscorner/detail/el/memo_16_2422

38. European Commission. The EU Cybersecurity Act. [Internet]. 2024 [cited 28 May 2025]; Available in:

https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

39. 2024 Global Chief Information Security Officer Organization and Compensation Survey. Heidrick & Struggles. [Internet]. 2024 [cited 28 May 2025]; Available in: https://www.heidrick.com/-/media/heidrickcom/publications-and-reports/2024-global-ciso-organization-and-compensation-survey.pdf

40. Safa NS, Von Solms R. An information security knowledge sharing model in organisations. Computers in Human Behaviour 2016;57:442–451. https://doi.org/10.1016/j.chb.2015.12.037

41. Safa NS, Von Solms R, Furnell S. Information security policy compliance model in organisations. Computers Security 2016;5670–82. https://doi.org/10.1016/j.cose.2015.10.006

42. Shameli-Sendi A, Aghababaei-Barzegar R, Cheriet M. Taxonomy of information security risk assessment (ISRA). Computers Security 2016;57:14–30. https://doi.org/10.1016/j.cose.2015.11.001

43. Shamala P, Ahmad R, Zolait A, Sedek M. Integrating information quality dimensions into information security risk management (ISRM). Journal of Information Security and Applications 2017;36:1–10. https://doi.org/10.1016/j.jisa.2017.07.004

44. International Organisation for Standardisation. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements. [Internet]. 2024 [cited 28 May 2025]; Available in: https://www.iso.org/standard/27001

45. Šikman L, Latinović T, Paspalj D. ISO 27001-Information Systems Security, development, trends, technical and economic challenges. Annals of the Faculty of Engineering Hunedoara [Internet]. 2019 [cited 28 May 2025];17(4):45–48. Available in: https://www.researchgate.net/publication/338585321

46. Alexei A. Ensuring information security in public organisations in the Republic of Moldova through the ISO 27001 standard. Journal of Social Sciences 2021;4(1):84–94. https://doi.org/10.52326/jss.utm.2021.4(1).11

47. Kamil Y, Lund S, Islam MS. Information security objectives and the output legitimacy of ISO/IEC 27001: stakeholders' perspective on expectations in private organisations in Sweden. Information Systems and e-Business Management 2023;21(3):699–722. https://doi.org/10.1007/s10257-023-00646-y

48. Culot G, Nassimbeni G, Podrecca M, Sartor M. The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. The TQM Journal 2021;33(7):76–105. https://doi.org/10.1108/TQM-09-2020-0202

49.The National Institute of Standards and Technology. Cybersecurity Framework. [Internet]. 2024 [cited 28 May 2025]; Available in: https://www.nist.gov/cyberframework

FINANCING

The authors did not receive financing for the development of this research.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

AUTHORSHIP CONTRIBUTION

Conceptualization: Anatolii Benzar.
Data curation: Artem Taranenko.
Formal analysis: Olha Balynska.
Research: Artem Taranenko.
Methodology: Yuliia Kovalenko.
Project management: Olha Balynska.
Resources: Artem Taranenko, Olha Balynska, Igor Balynskyi.
Software: Olha Balynska.
Supervision: Igor Balynskyi.
Validation: Igor Balynskyi.
Display: Igor Balynskyi.

Drafting - original draft: Anatolii Benzar, Yuliia Kovalenko.
Writing - proofreading and editing: Anatolii Benzar, Yuliia Kovalenko.

https://doi.org/10.62486/agma2025250 ISSN: 3046-4048