ENSURING INFORMATION SECURITY IN INSTITUTIONAL NETWORKS CONTEMPORARY CHALLENGES AND SOLUTIONS

Fiodor TIMERCAN
PhD Candidate, University Lecturer,
Department of Communications and Informatics,
"Alexandru cel Bun" Armed Forces Military Academy
E-mail: timercantudor@yahoo.com
ORCID: 0009-0001-6769-3556

Abstract: *The continuous digital transformation of institutional activity has significantly increased the dependence on computer networks for handling information resources. As a result, ensuring the security of information within institutional networks has become a fundamental requirement for the stable and reliable functioning of modern organizations. Institutions operate with diverse categories of data, including personal, administrative, and operational information, which require adequate protection against unauthorized access, loss, or compromise. This article addresses the issue of information security in institutional networks by analyzing the main challenges that arise in contemporary digital environments. The study outlines common sources of security risks, such as vulnerabilities in network infrastructures, improper access management, and insufficient awareness among users. At the same time, the paper discusses a set of practical solutions aimed at reducing these risks, with an emphasis on both technical safeguards and organizational measures. Special attention is paid to the necessity of integrating security technologies with institutional policies and procedures. The analysis highlights that effective information security cannot be achieved solely through technical means, but requires a systematic approach that includes risk assessment, staff training, and continuous monitoring of network activities. The conclusions drawn in this paper may serve as a reference for improving information security practices in educational and public institutions.*

Keywords: *information security; institutional networks; network protection; cybersecurity risks; security management.*

Classification JEL: *O3.*

UDC: *004.056.5:[37+351]* ***DOI:*** *https://doi.org/10.53486/ser2026.49*

1. Introduction

The rapid development of information and communication technologies has fundamentally changed the way institutions operate, manage resources, and interact with their internal and external environments. Computer networks have become an essential component of institutional infrastructures, supporting a wide range of activities, from administrative processes and educational services to data storage and information exchange. As institutions increasingly rely on digital systems, the volume and importance of information processed within institutional networks continue to grow.

This increased reliance on networked systems has also intensified concerns related to the security of information. Institutional networks frequently handle sensitive data, including personal information, internal documentation, and operational records, which must be protected against unauthorized access, alteration, or loss. In this context, information security is no longer a purely technical issue, but a complex organizational challenge that directly affects the continuity, credibility, and efficiency of institutional activity.

Modern institutional networks are exposed to a wide range of security threats. These threats originate from both external and internal sources and may include cyberattacks, exploitation

of software vulnerabilities, misconfiguration of network components, and human errors. The growing sophistication of cyber threats, combined with the increasing complexity of network infrastructures, makes it difficult for institutions to ensure an adequate level of protection using traditional security measures alone. Consequently, institutions are required to continuously reassess their approaches to information security and adapt them to evolving technological and organizational conditions (European Union Agency for Cybersecurity, 2023; MITRE Corporation, n.d.).

Another important aspect influencing information security in institutional networks is the human factor. Users often represent a critical link in the security chain, as insufficient awareness, lack of training, or improper use of information systems can create vulnerabilities that are easily exploited. In many cases, security incidents are not the result of advanced technical attacks, but rather of inadequate access control, weak authentication practices, or non-compliance with established security policies. This highlights the necessity of addressing information security not only through technological solutions, but also through effective management practices and user education (European Union Agency for Cybersecurity, 2019; National Cyber Security Centre, n.d.).

Ensuring information security in institutional networks requires a comprehensive and systematic approach. Technical measures such as access control mechanisms, encryption, network segmentation, and monitoring tools play a vital role in protecting information assets. However, their effectiveness largely depends on how well they are integrated into the institutional framework and supported by clear policies, procedures, and responsibilities. Information security management, therefore, becomes a key component in aligning technical safeguards with organizational objectives and regulatory requirements (International Organization for Standardization/International Electrotechnical Commission, 2022a; National Institute of Standards and Technology, 2024; ISACA, 2019).

In recent years, institutions have also faced increasing pressure to comply with legal and ethical standards related to data protection and privacy. Regulatory frameworks at national and international levels impose specific obligations on institutions regarding the handling of information, further emphasizing the importance of establishing reliable security practices. Failure to ensure adequate information security may result not only in operational disruptions, but also in legal consequences and reputational damage (European Union, 2016, 2022).

Within this context, the present study focuses on the issue of ensuring information security in institutional networks, with an emphasis on contemporary challenges and practical solutions. By examining common security risks and discussing relevant protective measures, the article aims to contribute to a clearer understanding of how institutions can strengthen their information security posture. The analysis is oriented toward educational and public institutions, but the observations and conclusions may also be applicable to other organizational environments that rely on networked information systems.

2. Literature Review

Information security in institutional networks is widely addressed in international standards, cybersecurity frameworks, and specialized literature. ISO/IEC 27001:2022 emphasizes the importance of implementing an information security management system based on risk assessment, security controls, monitoring, and continuous improvement. In the same direction, ISO/IEC 27002:2022 provides guidance on the selection and implementation of

information security controls (International Organization for Standardization/ International Electrotechnical Commission, 2022a, 2022b).

The NIST Cybersecurity Framework 2.0 highlights the need for a structured approach to cybersecurity management through the functions of govern, identify, protect, detect, respond, and recover. These functions are relevant for institutional networks because they support both preventive and corrective measures (National Institute of Standards and Technology, 2024).

ENISA reports also underline the evolution of the cyber threat landscape and the need for institutions to strengthen resilience, improve user awareness, and develop effective incident response capabilities. For educational and public institutions, these recommendations are especially important because such organizations manage sensitive data while also maintaining open access to digital services (National Cyber Security Centre, n.d.).

At the regulatory level, GDPR and the NIS2 Directive emphasize the obligation of institutions to protect personal data, ensure cybersecurity governance, and reduce operational risks (European Union, 2016, 2022). Therefore, the literature shows that information security must be approached as a combination of technical, organizational, legal, and human-centered measures.

3. Methodology

This study is based on a qualitative research approach, using conceptual analysis, documentary analysis, and synthesis of specialized literature. The research examines information security challenges in educational and public institutions by analyzing international standards, cybersecurity frameworks, regulatory documents, and relevant institutional practices (International Organization for Standardization/International Electrotechnical Commission, 2022a; National Institute of Standards and Technology, 2024).

The methodological approach includes the identification of common risks affecting institutional networks, the analysis of technical and organizational security measures, and the evaluation of their applicability in institutional environments. The study does not involve empirical data collection, but relies on the interpretation and comparison of existing theoretical and practical sources related to information security management (International Organization for Standardization, 2018; National Institute of Standards and Technology, 2012; Organisation for Economic Co-operation and Development, 2015).

This approach is appropriate because the objective of the article is to provide a structured understanding of contemporary cybersecurity challenges and to identify practical solutions that can be applied in educational and public institutional networks.

4. Results and Discussion

4.1. Specific security challenges in educational and public institutions

Educational and public institutions operate in a digital environment characterized by diversity, openness, and continuous interaction with a wide range of users. Unlike strictly controlled corporate or specialized networks, institutional networks in the public and educational sectors are designed to support accessibility, collaboration, and information exchange. While these characteristics are essential for fulfilling institutional missions, they

also introduce specific challenges related to information security (National Cyber Security Centre, n.d.; Organisation for Economic Co-operation and Development, 2015).

One of the defining features of educational and public institutions is the heterogeneity of their user base. Network access is typically granted to administrative staff, academic personnel, students, external collaborators, and, in some cases, the general public. This diversity complicates the implementation of uniform security controls and increases the likelihood of inconsistent security practices. Users often have varying levels of technical knowledge and awareness, which can result in unintentional security breaches caused by improper handling of information or misuse of network resources.

Another significant challenge is the coexistence of multiple categories of information within the same institutional network. Educational and public institutions manage personal data, academic records, financial information, internal communications, and publicly accessible content simultaneously. The need to balance openness and transparency with confidentiality and data protection creates a complex security landscape. In many cases, sensitive information is processed on the same infrastructure that supports public services, increasing the risk of data exposure if adequate segregation and protection mechanisms are not in place.

Institutional networks are also affected by resource constraints that influence information security practices. Budget limitations, insufficient technical staff, and aging infrastructure can hinder the adoption of advanced security technologies. As a result, institutions may rely on outdated systems or incomplete security solutions that are no longer adequate for addressing contemporary threats. These constraints are particularly evident in public and educational sectors, where investment in information security often competes with other institutional priorities.

The organizational structure of educational and public institutions further contributes to security challenges. Decision-making processes may be decentralized, with individual departments or units managing their own information systems. This fragmentation can lead to inconsistent security policies, overlapping responsibilities, and gaps in accountability. In the absence of centralized coordination, security measures may be implemented unevenly, reducing their overall effectiveness and increasing institutional exposure to risk.

External threats also play a critical role in shaping the security challenges faced by institutional networks. Publicly accessible systems are frequent targets for cyberattacks, including unauthorized access attempts, data extraction, and service disruption. Educational institutions, in particular, are often perceived as attractive targets due to their open environments and extensive user populations. The increasing availability of automated attack tools has lowered the barrier for malicious activities, making even moderately protected networks vulnerable (European Union Agency for Cybersecurity, 2023; MITRE Corporation, n.d.).

In addition to external threats, internal risks must be carefully considered. Insider threats, whether intentional or accidental, represent a significant source of security incidents in institutional environments. Weak access controls, shared credentials, and insufficient monitoring can enable unauthorized actions that compromise information security. These risks are exacerbated in institutions where security responsibilities are not clearly defined or where compliance with security policies is not actively enforced.

Legal and regulatory requirements add another layer of complexity to information security in educational and public institutions. Regulations related to data protection and privacy

impose specific obligations regarding the collection, processing, and storage of information. Ensuring compliance requires not only technical safeguards, but also well-defined procedures and documentation. Failure to meet these requirements may result in legal consequences and loss of public trust, further emphasizing the importance of robust security practices (European Union, 2016, 2022).

Taken together, these factors illustrate that information security challenges in educational and public institutions are multidimensional and closely linked to organizational, technical, and human elements. Addressing these challenges requires a comprehensive understanding of the institutional context and the constraints under which networks operate. Recognizing the specific characteristics of educational and public environments is a necessary step toward developing effective and sustainable information security solutions.

Figure 1 illustrates a conceptual architecture of information security in institutional networks, emphasizing the layered nature of protection mechanisms. The model shows how technical controls, such as network defenses and access management, operate together with organizational policies and monitoring processes to protect information assets. Each layer addresses specific security functions, contributing to the protection of confidentiality, integrity, and availability of information.

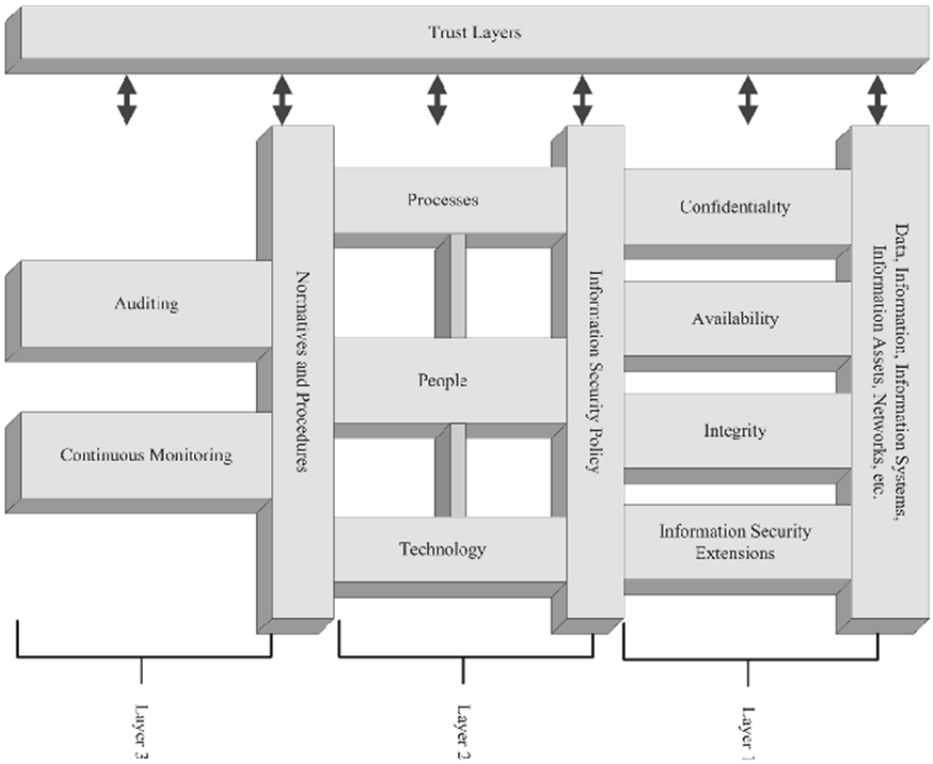

Figure 1. Information security architecture.
***Source**: Author's elaboration.*

The figure also highlights the importance of coordination between technological solutions and institutional procedures. By integrating preventive, detective, and corrective measures, the architecture reflects a comprehensive approach to information security that is particularly relevant for educational and public institutions, where network accessibility must be balanced with data protection requirements.

4.2. Implementation of information security measures in institutional networks

The implementation of information security measures in institutional networks represents a complex and continuous process that must take into account both the specific characteristics of the institutional environment and the evolving nature of cyber threats. Unlike theoretical security models, practical implementation requires adapting general security principles to concrete organizational structures, available resources, and operational requirements. In educational and public institutions, this process is further influenced by the need to maintain accessibility and functionality while ensuring adequate protection of information assets.

A fundamental aspect of implementing information security measures is the establishment of clear access control mechanisms. Institutional networks typically support a large number of users with different roles and responsibilities, making it essential to define access rights in accordance with the principle of least privilege. Users should be granted access only to the information and systems necessary for the performance of their tasks. Proper authentication methods, combined with role-based access control, reduce the risk of unauthorized access and limit the potential impact of security incidents (Center for Internet Security, n.d.; Cybersecurity and Infrastructure Security Agency, 2023b; International Organization for Standardization/International Electrotechnical Commission, 2022b).

Network segmentation constitutes another important measure in securing institutional infrastructures. By separating network resources into distinct segments based on function or sensitivity, institutions can reduce the spread of security incidents and improve control over data flows. Segmentation allows sensitive systems and data repositories to be isolated from publicly accessible services, thereby minimizing exposure to external threats. In institutional environments, this approach supports a balanced coexistence of open services and protected internal resources (Cybersecurity and Infrastructure Security Agency, 2023b; National Institute of Standards and Technology, 2020).

Encryption technologies play a key role in protecting information during storage and transmission. Implementing encryption for sensitive data helps prevent unauthorized disclosure, even in cases where network defenses are breached. In institutional networks, encryption is particularly relevant for protecting personal data, internal communications, and confidential records. The effective use of encryption requires not only appropriate technical solutions, but also clear policies regarding key management and data handling procedures (European Union, 2016; International Organization for Standardization/International Electrotechnical Commission, 2022b; National Institute of Standards and Technology, 2020).

Monitoring and incident detection mechanisms are essential components of information security implementation. Continuous monitoring of network activity enables institutions to identify abnormal behavior, potential intrusions, and policy violations in a timely manner. Intrusion detection and logging systems provide valuable information for responding to incidents and improving security controls. However, the effectiveness of these mechanisms depends on the ability of institutions to analyze collected data and act upon identified risks (Cybersecurity and Infrastructure Security Agency, 2023a; MITRE Corporation, n.d.; National Institute of Standards and Technology, 2024).

Beyond technical measures, organizational and procedural aspects play a decisive role in the successful implementation of information security. Security policies and procedures establish a

common framework for acceptable use of network resources and define responsibilities related to information protection. These documents serve as a reference for both users and administrators and contribute to consistency in security practices across the institution. Without clear policies, technical measures may be applied inconsistently or misunderstood by users.

Staff training and awareness initiatives represent another critical element of implementation. Users are often the first line of interaction with information systems, and their behavior can significantly influence security outcomes. Regular training programs help users understand potential risks, recognize security threats, and comply with institutional security requirements. In educational and public institutions, fostering a culture of security awareness is essential for reducing human-related vulnerabilities (European Union Agency for Cybersecurity, 2019; National Cyber Security Centre, n.d.).

The implementation of information security measures must also include mechanisms for regular evaluation and improvement. Security solutions that are effective at one point in time may become insufficient as technologies and threats evolve. Periodic assessments, audits, and risk analyses enable institutions to identify weaknesses and adjust their security strategies accordingly. This iterative approach supports long-term resilience and helps institutions maintain an appropriate level of protection.

Overall, implementing information security measures in institutional networks requires a coordinated effort that integrates technical solutions with organizational practices and human factors. Effective implementation is not achieved through isolated actions, but through a structured and adaptable process aligned with institutional goals and constraints. Such an approach allows educational and public institutions to address security challenges while preserving the openness and functionality that characterize their digital environments.

Figure 2. Multi-Layer Security Architecture

***Source**: Author's elaboration based on ISO/IEC 27001:2022, NIST Cybersecurity Framework 2.0, GDPR, and NIST Cybersecurity Framework 2.0.*

Figure 2 presents a multi-layer security architecture model that integrates several protective components working together to safeguard institutional networks. The architecture highlights how layered defenses help protect information assets by combining perimeter defenses, access controls, encryption, monitoring, and governance mechanisms into a coherent framework. Each layer corresponds to a category of security controls that collectively enhance the confidentiality, integrity, and availability of data.

The model underscores the interaction between technical controls and organizational policies. It shows that while technical elements such as firewalls, intrusion detection systems, and encryption form essential protective layers, their effectiveness depends on how well they are supported by institutional procedures, user awareness, and continuous monitoring. This layered view reflects the idea that no single control is sufficient in isolation and that robust information security requires coordinated, multi-level protection.

The model is particularly relevant for educational and public institutions, where open access and diverse user populations increase exposure to security risks, and a structured, layered security approach can help balance openness with effective data protection.

4.3. Evaluation of information security effectiveness

The evaluation of information security effectiveness in institutional networks constitutes a complex analytical process through which institutions can understand the real impact of security measures on their digital environments. In educational and public institutions, information systems support not only administrative and operational activities, but also teaching, research, communication, and public services. Under these conditions, evaluation becomes essential for determining whether implemented security mechanisms genuinely contribute to institutional stability or merely create a formal appearance of protection.

Assessing security effectiveness requires an understanding of institutional objectives and operational constraints. Unlike environments governed exclusively by efficiency or profit considerations, institutional networks must support accessibility, openness, and continuity of services. Evaluation therefore cannot be reduced to the simple measurement of technical performance indicators. It must also consider how security measures influence everyday activities, user behavior, and the overall functionality of the institutional infrastructure. Security solutions that are technically robust but poorly aligned with institutional practices may generate workarounds that ultimately weaken protection.

From a technical standpoint, evaluation involves detailed examination of network components, system configurations, access mechanisms, and data handling practices. Institutional networks often evolve incrementally, incorporating legacy systems alongside newer technologies. This heterogeneity increases the likelihood of configuration inconsistencies and hidden vulnerabilities. Through systematic analysis of system logs, access records, and network traffic patterns, institutions can identify weaknesses that do not immediately manifest as incidents but represent latent risks. Such evaluations provide insight into how well security controls perform under real operational conditions, rather than under assumed or ideal scenarios.

Evaluation at the network level also requires attention to interactions between systems managed by different organizational units. In many institutions, responsibility for information systems is distributed across departments, faculties, or administrative divisions. This decentralization can result in fragmented security practices and uneven application of controls. Evaluating the coherence of security measures across the entire network allows

institutions to identify structural gaps, overlapping responsibilities, and inconsistencies that may compromise overall security effectiveness.

Organizational aspects form an equally important part of the evaluation process. Policies, procedures, and governance structures define how security is implemented and enforced in practice. Evaluating these elements involves examining whether security responsibilities are clearly assigned, whether decision-making processes support timely responses to emerging risks, and whether established procedures are realistically applicable in daily operations. In institutional contexts, security failures often stem from ambiguity in roles or insufficient coordination rather than from purely technical shortcomings.

The human dimension of security evaluation is particularly significant in educational and public institutions due to the diversity and fluidity of user populations. Staff members, students, external collaborators, and visitors interact with institutional networks in different ways and with varying levels of awareness. Evaluating the effectiveness of training initiatives, awareness programs, and communication strategies helps institutions understand how security requirements are interpreted and applied by users. Patterns of behavior observed during evaluation can reveal misunderstandings, informal practices, or habitual actions that increase exposure to risk, even when formal policies exist.

Risk-oriented evaluation provides a broader analytical perspective by linking security performance to potential consequences. Institutional environments are subject to changing threat landscapes, technological developments, and regulatory expectations. Evaluation processes must therefore consider not only current vulnerabilities, but also the institution's capacity to adapt to new risks. By correlating evaluation findings with risk assessments, institutions can prioritize improvements and allocate resources in a manner consistent with their strategic objectives and tolerance for disruption (International Organization for Standardization, 2018; National Institute of Standards and Technology, 2012; Organisation for Economic Co-operation and Development, 2015).

Security incidents represent another valuable source of evaluative information. Even incidents with limited impact can reveal important insights into the adequacy of detection mechanisms, response procedures, and recovery capabilities. Evaluating how incidents are identified, reported, and addressed allows institutions to assess the practical effectiveness of their security frameworks. This analysis supports institutional learning and contributes to the gradual refinement of preventive and corrective measures (Cybersecurity and Infrastructure Security Agency, 2023a; National Institute of Standards and Technology, 2024).

Evaluation also plays a role in supporting accountability and transparency within institutional structures. Documented evaluation outcomes provide a basis for informed decision-making at the management level and support compliance with legal and regulatory obligations related to data protection and information security. In public and educational institutions, such documentation also contributes to maintaining trust among stakeholders by demonstrating a systematic approach to safeguarding information resources.

Viewed in its entirety, the evaluation of information security effectiveness in institutional networks is an ongoing and integrative process that combines technical analysis, organizational assessment, and examination of human factors. It enables institutions to move beyond reactive responses to security incidents and toward a more reflective and adaptive approach to security management. Through sustained and context-aware evaluation

practices, institutions can strengthen the resilience of their network infrastructures while preserving the openness and functionality essential to their missions.

5. Conclusions

The analysis presented in this article highlights the complexity of ensuring information security within institutional networks and emphasizes the necessity of addressing this issue through an integrated and context-aware approach. Educational and public institutions operate in digital environments characterized by openness, diversity of users, and evolving technological infrastructures, which creates specific challenges that cannot be effectively managed through isolated technical solutions.

The examination of security challenges demonstrates that institutional networks are exposed to a broad spectrum of risks arising from technical vulnerabilities, organizational constraints, and human behavior. These risks are closely interconnected and often reinforced by limited resources, decentralized management structures, and heterogeneous information systems. As a result, information security in institutional environments must be understood as a multidimensional responsibility rather than a purely technical task.

The discussion on the implementation of security measures shows that effective protection depends on the alignment of technological safeguards with institutional policies and operational practices. Access control mechanisms, network segmentation, encryption, and monitoring tools provide essential protection only when they are embedded within clear procedures and supported by informed and responsible users. In institutional contexts, where accessibility and functionality are critical, security measures must be designed to support rather than hinder legitimate activities.

The evaluation of information security effectiveness emerges as a key element for maintaining and improving institutional security postures. Continuous assessment of technical performance, organizational arrangements, and user behavior enables institutions to identify weaknesses, adapt to changing risks, and refine security strategies over time. Evaluation supports informed decision-making, strengthens accountability, and contributes to institutional resilience in the face of evolving threats.

Taken together, the findings of this study indicate that sustainable information security in institutional networks requires a balanced combination of technical, organizational, and human-centered measures. Institutions that adopt a systematic and adaptive approach to security management are better positioned to protect information assets while preserving the openness and trust essential to their missions. Further research may focus on developing evaluation frameworks tailored to specific institutional contexts and on exploring practical methods for integrating security awareness into everyday institutional practices.

7. References

Center for Internet Security. (2024). *CIS critical security controls version 8.1*. https://www.cisecurity.org/controls/v8-1

Cybersecurity and Infrastructure Security Agency. (2023a). *Cross-sector cybersecurity performance goals*. https://www.cisa.gov/cross-sector-cybersecurity-performance-goals

Cybersecurity and Infrastructure Security Agency. (2023b). *Zero trust maturity model: Version 2.0*. https://www.cisa.gov/sites/default/files/2023-04/CISA_Zero_Trust_Maturity_Model_Version_2_508c.pdf

European Union. (2016). *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*. Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2016/679/oj

European Union. (2022). *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union*. Official Journal of the European Union. https://eur-lex.europa.eu/eli/dir/2022/2555/oj

European Union Agency for Cybersecurity. (2019). *Cybersecurity culture guidelines: Behavioural aspects of cybersecurity*. https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity

European Union Agency for Cybersecurity. (2023). *ENISA threat landscape 2023*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

International Organization for Standardization. (2018). *Risk management — Guidelines* (ISO Standard No. 31000:2018). https://www.iso.org/standard/65694.html

International Organization for Standardization & International Electrotechnical Commission. (2022a). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements* (ISO/IEC Standard No. 27001:2022). https://www.iso.org/standard/27001

International Organization for Standardization & International Electrotechnical Commission. (2022b). *Information security, cybersecurity and privacy protection — Information security controls* (ISO/IEC Standard No. 27002:2022). https://www.iso.org/standard/75652.html

ISACA. (2019). *COBIT 2019 framework: Governance and management objectives*. https://www.isaca.org/resources/cobit

MITRE Corporation. (n.d.). *MITRE ATT&CK*. Retrieved June 3, 2026, from https://attack.mitre.org/

National Cyber Security Centre. (n.d.). *Cyber security for schools*. Retrieved June 3, 2026, from https://www.ncsc.gov.uk/section/education-skills/cyber-security-schools

National Institute of Standards and Technology. (2012). *Guide for conducting risk assessments* (Special Publication 800-30, Rev. 1). https://csrc.nist.gov/pubs/sp/800/30/r1/final

National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations* (Special Publication 800-53, Rev. 5). https://csrc.nist.gov/pubs/sp/800/53/r5/final

National Institute of Standards and Technology. (2024). *The NIST cybersecurity framework (CSF) 2.0* (NIST CSWP No. 29). https://doi.org/10.6028/NIST.CSWP.29

Organisation for Economic Co-operation and Development. (2015). *Digital security risk management for economic and social prosperity: OECD recommendation and companion document*. OECD Publishing. https://doi.org/10.1787/9789264245471-en