**Evaluation of Information Security Practices in the Context of Digital Transformation**

**Abstract.** Digital transformation is accelerating the adoption of cloud platforms, data-intensive services and IoT ecosystems, reshaping the attack surface organisations must defend. This study provides an integrated assessment of information-security maturity in that context. Using a multi-method design—systematic literature review, cross-sector case studies, comparative analysis of leading maturity frameworks (NIST CSF, COBIT, CMMI, CMAF), and an expert survey—we gauge how well current controls, processes, and cultures align with emerging risks. Quantitative benchmarking indicates that enterprises operating at maturity levels 4–5 experience ≈50 % fewer major breaches than peers at levels 1–3, yet fewer than one-third routinely rehearse cloud- and IoT-oriented attack scenarios, exposing a persistent threat–readiness gap. To bridge this gap, the paper proposes an adaptive governance model that couples zero-trust principles and ML-driven analytics with continuous risk appraisal and culture-centric interventions. The findings inform security leaders and policymakers where to prioritise investment, emphasising that sustained digital growth depends on embedding cybersecurity maturity as a core metric of organisational resilience.

**Keywords:** digital transformation; cybersecurity maturity; information-security governance; risk management; organisational resilience; cloud security; IoT threats.

**Introduction**

In an era of rapid technological transformation, digital-security concerns have become fundamental for both individual organizations and entire economic systems globally, as the explosive growth of data volumes, the expansion of digital platforms, the widespread adoption of cloud solutions, and the integration of intelligent algorithms have fundamentally reshaped the principles of storing, processing, and protecting information assets. Under such a large-scale technological shift, there is an increasing need for a robust information-security architecture capable of guaranteeing the confidentiality, integrity, and availability of information resources while ensuring the resilience of strategically critical business functions.

According to the provisions of ISO/IEC 27000, the concept of information security encompasses not only the state of protection but also the full set of technical, regulatory, and managerial mechanisms designed to reduce the likelihood of information distortion, blocking, loss, or uncontrolled dissemination. In practice, this requires establishing an end-to-end, scalable, and adaptive digital-protection system that must include components for access control, incident response, cryptographic protocols, a regulatory framework, independent auditing, and qualified personnel support.

Heightened focus on digital security stems not only from the necessity of internal risk management but also from external realities: the activation of cybercriminal organizations and the increasing scale of attacks on digital infrastructure complicate threat forecasting and dramatically amplify potential damage. Research by leading analytical agencies emphasizes that threats to cloud systems, compromises of third-party services, breach-and-leak operations, and intrusions into IoT environments provoke the greatest concern while organizations remain least prepared. This imbalance between threat severity and defensive readiness underscores the need to rethink digital-security strategies and to significantly increase investments in resilience-enhancing measures.

The transition to a digital model—initially conceived as a limited push toward automation—had, by the mid-2020s, evolved into a systematic redesign of all sectors: from finance and healthcare to public administration and the service economy, characterized by the predominance of cloud solutions, platform-based architectures, remote collaboration, intelligent analytics, telecommunications-enabled public services, and telemedicine. This acceleration under pandemic conditions proceeded with insufficient attention to digital-security principles, resulting in a broad spectrum of vulnerabilities: configuration errors, exposed API endpoints, outdated access-control mechanisms, and obsolete protection methods.

**Materials and Methods**

The article by Ahmad, Maulana, and Yassir [1] presents a comprehensive analysis of key cybersecurity challenges in the context of the digital transformation of information systems. It emphasizes the vulnerabilities emerging from the integration of new technologies and underlines the necessity of building resilient information security architectures in a rapidly evolving digital environment. The study by Zielińska, Nowak, and Lis [2] explores cybersecurity threats from a strategic management perspective in digital innovation, highlighting the need for an interdisciplinary approach to risk management in organizations implementing digital solutions. The work by Cherkaoui, Rachidi, and El Koutbi [3] examines the interplay between digital transformation and the increasing complexity of cyber threats, with particular attention to preventive measures and counterstrategies that should be applied to mitigate evolving risks. The methodology proposed by Klishin and Chechulin [4], presented in Springer’s *Lecture Notes in Electrical Engineering*, focuses on analyzing the impact of digital transformation of information security management processes on enterprise architecture, emphasizing the importance of structural alignment between IT solutions and security frameworks.

The framework introduced by Liyanage, Archchilage, and Russello [5] proposes a novel approach to assessing cybersecurity maturity levels in organizations. It is based on multilayered metrics and integration with existing risk management processes, enabling tailored protective measures aligned with digital strategies. The publication by Lysenko et al. [6] investigates the management of cybersecurity risks in the era of digital transformation, stressing the significance of flexible and adaptive policies in response to the evolving threat landscape. Peterson’s study [7] analyzes the impact of national cybersecurity policies on digital transformation initiatives, emphasizing the importance of synchronizing regulatory frameworks with technological advancements. The analytical report by PwC [8] provides a global perspective on digital trust trends, highlighting the critical role of resilience in digital enterprises amidst growing interconnectivity and dependence on IT infrastructures. The development by Rahman and colleagues [9] introduces *AssessITS*, a tool that integrates procedural guidelines and practical evaluation metrics for IT and cybersecurity risk assessment in organizations, offering a standardized yet adaptable approach to building secure digital environments. The work by Saeed et al. [10] discusses current challenges in ensuring cybersecurity during business digital transformation, focusing on enhancing resilience through technological innovation and institutional mechanisms.

This research employs a multi-method approach: a literature review to identify current challenges and frameworks; case-study analysis to examine organizational practices; comparative analysis of cybersecurity-maturity models; expert surveys to capture up-to-date information-security practices; quantitative evaluation of defense-measure effectiveness; and risk-management process modeling under digital-transformation conditions. Such a comprehensive methodology enables a thorough assessment of existing practices and the identification of avenues for their enhancement.

**Results and Discussion**

Information security is defined as the condition in which data confidentiality, integrity, and availability are maintained, and processing workflows remain uncompromised. According to ISO/IEC 27000, this concept encompasses the full suite of technical, managerial, regulatory, and personnel measures aimed at reducing the likelihood of data loss through leakage, falsification, destruction, or blocking [1]. The modern data-protection perimeter comprises the following principal domains: threat management through identification, analysis, and mitigation; definition of access-control policies for information assets; incident-logging and response mechanisms; deployment of technical solutions (including firewalls, antivirus software, and intrusion-prevention systems); organizational instruments (procedures, policies, and regulations); and continuous personnel training [4]. In the context of the global proliferation of digital services, cloud infrastructure, IoT deployments, and the large-scale expansion of remote work, information-security breaches carry significant economic costs, erode customer trust, weaken competitive standing, and even pose national-security risks [2].

Digital transformation entails a systemic, sustained overhaul of social, economic, and administrative processes, driven by the widespread adoption of digital solutions. This acceleration commenced in the 2010s and became particularly pronounced under pandemic constraints, when migrations to cloud and platform-based architectures were executed in timeframes originally projected for years [3]. Core trajectories of digital transformation include:

* Automation of logistics operations and digitalization of sales channels in the private sector.
* Implementation of electronic registries and online services in government administration;
* Development of telemedicine and analytics within healthcare systems;
* Remote learning formats in education;
* Mobile payments, digital banking, and blockchain applications in finance [7].

The impact of digital transformation is dual: it enhances convenience, accelerates operations, and reduces costs, yet also expands vulnerability surfaces, increases attack vectors, and necessitates reconfiguration of security architectures to address new technological realities [6]. Although rapid digitalization delivers clear advantages, it simultaneously yields both productive and destructive consequences for information security. Table 1 organizes these effects according to key security principles.

*Table 1. Effects of Rapid Digitalization on Information Security (Compiled by the author based on original research)*

| **Positive Effects** | **Negative Effects** |
| --- | --- |
| Increased automation and faster incident response | Growth in vulnerabilities within new digital services and platforms |
| Deployment of modern information-security technologies | Insufficient maturity of security systems amid accelerated integration |
| Expanded threat monitoring and analytics | Human factor—insufficient employee preparedness |
| Standardization and digitalization of security controls | Increased workload for security teams |
| Enhanced remote management, regulation, and protection | Expanded attack surface due to the connectivity of new devices |
| Integration of information security into strategic management | Regulatory framework lagging behind the pace of digitalization |

Digitalization presents organizations with extensive opportunities to strengthen cybersecurity measures, but when accelerated without due care, it can introduce new vulnerabilities. Mitigating these risks requires a calibrated strategy: phased deployment, targeted personnel training, the development of regulatory frameworks, and the institutional reinforcement of information-security policy [3].

In an environment of rapid technological renewal and a surging volume of cyberthreats, information protection demands a comprehensive, multilayered, structured approach. In practice, this manifests as a cohesive set of diverse methods grouped into four distinct domains—technical mechanisms; organizational and regulatory tools; threat-assessment and audit systems; and next-generation intelligent, adaptive technologies—each playing a defining role in building a resilient, flexible security posture [10].

The technical domain encompasses cryptographic mechanisms—encryption tools, digital keys, and authentication/authorization technologies (including biometric systems)—alongside network-flow protection via VPNs, firewalls, and intrusion-detection/prevention systems (IDS/IPS), supplemented by antivirus, backup solutions, anti-phishing measures, and post-incident recovery processes. The effectiveness of these controls hinges on their up-to-date configuration, seamless integration, and governance [5].

The second domain focuses on cyber-security policy development: drafting internal regulations, conducting systematic employee training, clearly delineating roles, establishing incident-response processes, and implementing an information-security management system (ISMS) in line with international standards such as ISO/IEC 27001—which, according to ISACA, can halve the likelihood of serious incidents and thus occupies a central position in digital-strategy planning [8].

The analytical domain relies on regular risk assessments, infrastructure audits, and penetration testing using models like CRAMM, FAIR, or OCTAVE. These frameworks reveal potential vulnerabilities, estimate probable losses, and enable prioritized safeguards—enhancing system transparency and the rationale for decision-making [1].

The fourth domain marks the shift to agile, intelligence-driven architectures: embracing Zero-Trust principles, behavioral-analysis algorithms, and machine-learning systems capable of detecting suspicious activity in real time and automatically triggering countermeasures. This greatly bolsters cyber-resilience and minimizes response lag in the face of evolving threats (see Table 2).

*Table 2. Information-Security Practices under Digital Transformation (compiled by the author)*

| **Practice** | **Advantages** | **Disadvantages** |
| --- | --- | --- |
| IS policy and ISMS implementation | Systematic approach; standards compliance | Complexity of rollout; procedural rigidity |
| Cryptography | Robust data protection | Key-management challenges |
| IDS/IPS systems | Real-time attack detection | False positives; requires frequent updates |
| AI and behavioral analysis | Adaptable to emerging threats | Data-dependent; potential for errors |
| Personnel training | Reduces human-factor risk | Requires regular repetition; variable efficacy |
| Risk assessment | Helps prioritize defenses | Dependent on data quality |
| Zero Trust | Trustless access control | Complex and costly to implement |

Thus, ensuring stable protection in the digital age requires a blend of varied strategies, flexibly aligned with an organization’s specific risk profile and resource capacity [2]. Only a coordinated fusion of technical controls, organizational-regulatory foundations, continuous risk monitoring, and intelligent solutions can deliver a dependable, adaptive, and modern information-security model [4].

Digital transformation demands a fundamental reappraisal of traditional conceptions of information security. In an environment of rapid technological shifts and exponentially growing data volumes, the critical value lies not merely in deploying protective mechanisms but in conducting regular, systematic diagnostics of security practices’ effectiveness and maturity. To this end, maturity models are employed that quantitatively and qualitatively depict the current level of development and highlight areas for optimization [9].

Despite the ongoing evolution of digital security measures, organizations confront increasingly chaotic and unpredictable challenges. The expanding attack surface—driven by reliance on cloud platforms, artificial‐intelligence algorithms, interconnected devices, and third-party vendors—necessitates a flexible, comprehensive resilience strategy. Synchronizing priorities and preparedness levels across the organizational hierarchy is essential to maintaining security posture and business continuity (see Figure 1).

**

*Figure 1. Relationship between Concern over Cyber Threats and Level of Cyber Readiness [8]*

Organizations express greatest anxiety about those threats against which they feel least prepared—namely, attacks targeting cloud infrastructure, unauthorized access leading to data exfiltration, partner-mediated compromises, and IoT intrusions. These very threat categories exhibit the lowest internal readiness among security teams, underscoring the need for targeted investments and reinforced incident-response capabilities [6].

Among the established tools for evaluating cybersecurity process maturity, the following frameworks hold central importance:

* CMMI: a universal integration framework adapted to assess the systemic coherence and manageability of security activities;
* COBIT: an instrumental approach for IT-resource governance and risk assessment within an enterprise‐wide security architecture;
* CMAF: a compliance and threat-preparedness analysis framework;
* NIST Cybersecurity Framework: covering the full spectrum of security—asset identification, preventive measures, detection, response, and recovery—which, owing to its comprehensive structure, is widely adopted in both private and public sectors [5].

Each model furnishes organizations with objective benchmarks for analyzing current capabilities, uncovering vulnerabilities, and designing improvement plans—an imperative in light of accelerating threat and system transformations [6].

According to PwC data for 2021–2024, enterprises scoring high on maturity (levels 4–5 on a five-point scale) experience major security incidents at half the rate of less mature peers. However, widespread digitalization has surfaced acute challenges: existing policies often fail to address new digital workflows; regulatory updates lag behind technological change; many organizations continue to rely on outdated solutions ill-suited for modern architectures; and fewer than one-third conduct regular threat-scenario simulations [8]. These findings indicate that effective protection requires more than a one-off maturity assessment—it demands a dynamic governance system with periodic strategy adjustments in response to both technological advances and regulatory developments.

**Conclusion**

In an environment of rapid technological renewal, digital security has become an indispensable component of organizational resilience. Ubiquitous integration of cloud solutions, intelligent systems, networked devices, and external providers—while enhancing operational efficiency—simultaneously multiplies the corporate infrastructure’s exposure to external threats. Notably, those vectors that cause the greatest concern—unauthorized interventions in cloud platforms, partner-related compromises, illicit access followed by data exfiltration, and IoT-ecosystem destabilization—are also the areas in which corporate readiness is lowest, underscoring the urgent need to rethink the foundations of a resilient digital environment.

This misalignment between the intensity of threats and the level of preparedness demands a systemic revision of cyber-resilience strategies. Technological upgrades alone are insufficient; organizations must foster a culture of digital accountability, implement continuous training programs for staff, reinforce risk-management frameworks, and direct investments toward the long-term maturity of information-security systems. Applying maturity models such as NIST and COBIT helps structure these initiatives, concentrate resources on the most vulnerable areas, and chart a deliberate path toward enhanced internal resilience, thereby establishing a robust framework for critical-risk management.

Looking ahead, emerging paradigms will further redefine the security landscape. The imminent advent of practical quantum computing threatens to break today’s public-key cryptography; therefore, roadmaps must already include pilot deployments of post-quantum algorithms and, where feasible, quantum-key-distribution (QKD) channels for high-value links. In parallel, zero-knowledge proofs (ZKPs) are maturing into viable building blocks for privacy-preserving authentication, regulatory compliance and secure multiparty computation—allowing organisations to verify transactions or data properties without exposing the underlying data itself. Incorporating these technologies early mitigates future cryptanalytic shocks, satisfies tightening privacy mandates and positions enterprises at the forefront of secure digital-economy practices.

Digital protection today transcends a purely technical domain to assume the status of a strategic function that pervades every organisational layer—from frontline teams to business units and executive leadership. Synchronising priorities across technical departments, senior management, and operational units is essential for maintaining resilience, safeguarding corporate interests, and building stakeholder trust. Neglecting this integrated approach exposes organisations to legal, economic, and reputational risks capable of destabilising operations and inflicting irreparable harm—particularly amid tightening regulatory regimes and ever-more sophisticated cyberattacks. Only a comprehensive, proactive posture—combining mature governance, adaptive technological solutions, post-quantum preparedness, and privacy-centric protocols such as ZKPs—can secure competitive advantage and reliable protection in today’ and tomorrow’s swiftly evolving digital landscape.

Author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, manuscript.

**References**

1. Ahmad, S., Maulana, I., & Yassir, M. (2024). Cybersecurity challenges in the era of digital transformation: A comprehensive analysis of information systems. JIEM.<https://www.researchgate.net/publication/378295876_Cybersecurity_Challenges_In_The_Era_Of_Digital_Transformation_A_Comprehensive_Analysis_Of_Information_Systems>
2. M. Zielińska,Nowak, T., & K. Lis, (2024). Cybersecurity challenges in digital innovation: A strategic management perspective. Digital Innovation: International Journal of Management.<https://international.arimbi.or.id/index.php/DigitalInnovation/article/view/155>
3. Cherkaoui, S., Rachidi, T., & El Koutbi, M. (2021). Digital transformation, cybersecurity challenges, and countermeasures. Turkish Online Journal of Qualitative Inquiry, 12(5), 5519–5534.<https://www.tojqi.net/journal/index.php/TOJQI/article/view/5015>
4. Klishin, D., & Chechulin, A. (2024). Methodology for analyzing the impact of digital transformation of the information security management process on the enterprise architecture. In Lecture Notes in Electrical Engineering. Springer.<https://www.researchgate.net/publication/377108451_Methodology_for_Analyzing_the_Impact_of_Digital_Transformation_of_the_Information_Security_Management_Process_on_the_Enterprise_Architecture>
5. Liyanage, S., Archchilage, N., & Russello, G. (2025). A novel framework to assess cybersecurity capability maturity. arXiv.<https://arxiv.org/abs/2504.01305>
6. S. Lysenko, O. Verba, V. Kyrychenko, V. Gandziuk, I. Odobetska (2025). Managing cybersecurity risks in the era of digital transformation. Journal of Information Systems Engineering and Management.<https://jisem-journal.com/index.php/journal/article/view/330>
7. Peterson, V. (2024). Cybersecurity policies and their impact on national digital transformation initiatives. Journal of Applied Cybersecurity Analytics.<https://www.researchgate.net/publication/387335771_Cybersecurity_Policies_and_Their_Impact_on_National_Digital_Transformation_Initiatives>
8. PwC. (2024). Global Digital Trust Insights 2024: Toward the resilient digital enterprise.<https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html>
9. Rahman, M. & Others. (2024). AssessITS: Integrating procedural guidelines and practical evaluation metrics for organizational IT and cybersecurity risk assessment. arXiv.<https://www.researchgate.net/publication/384599117_AssessITS_Integrating_procedural_guidelines_and_practical_evaluation_metrics_for_organizational_IT_and_Cybersecurity_risk_assessment>
10. S.Saeed & Others. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. Sensors (Basel), 23(15).<https://www.mdpi.com/1424-8220/23/15/6666>