Gradus Vol 13, No 1 (2026)
ISSN 2064-8014

IT GOVERNANCE AND INFORMATION SECURITY GOVERNANCE SYNERGIES ARISING FROM TODAY'S CHALLENGES

Gábor Zsolt Kiss[1,*]

[1] Doctoral School of Public Administration Sciences, Faculty of Public Governance and International Studies, Ludovika-University of Public Service, Hungary, https://orcid.org/0009-0004-4314-903X

https://doi.org/10.47833/2026.1.CSC.001

Keywords:
IT Governance
Information Security Governance
Regulation
Risk Management
Compliance

Article history:
Received 12 Nov 2025
Revised 28 Jan 2026
Accepted 1 Febr 2026

Abstract

Digitalisation and the increasing complexity of organisational information systems have brought IT governance and information security governance into closer alignment. This study examines how evolving technological risks and recent European regulatory measures – including GDPR, NIS2 and DORA – shape governance expectations and reinforce the need for coordinated oversight. Drawing on established frameworks such as COBIT, ITIL and ISO/IEC 27001, the paper identifies the main points of interaction between IT and security governance. It highlights the benefits of integrated, risk-based practices. The findings show that unified governance structures improve strategic alignment, strengthen risk management and compliance, and support more resilient operational performance in complex digital environments.

1 Introduction

By the mid-2020s, the operational environment of organisations will have been substantially reshaped by the rapid expansion of digital infrastructures, cloud-based services, and interconnected devices. Contemporary information systems function as interdependent information systems, where reliability and security directly influence organisational performance, continuity, and public confidence. As system architectures become more intricate, the governance structures responsible for oversight face greater expectations to ensure that technological development remains aligned with risk management requirements. Information security, previously regarded primarily as a technical safeguard, has become a central element of strategic management.

Recent incidents across several critical sectors show a clear progression toward more organised, technically sophisticated attack methods.

Incidents affecting critical services, cloud environments, and supply chains show that vulnerabilities often arise not only from technical weaknesses but also from shortcomings in governance, coordination, and risk ownership. Threat actors now operate with substantial resources, employing methods that extend beyond traditional intrusion techniques to include disruption and extortion that may affect core business processes. These developments emphasise the need for governance structures that integrate security considerations across all stages of the IT service lifecycle.

Recent EU regulatory measures, including NIS2 and DORA, have broadened organisational obligations concerning digital operational resilience and security. The introduction of the NIS2 Directive, the Digital Operational Resilience Act (DORA), and related measures reflects a move toward greater transparency and accountability, harmonised security requirements, and more systematic risk management practices. These instruments require organisations to demonstrate

* Corresponding author.
E-mail address: kiss.gabor.zsolt@stud.uni-nke.hu

operational resilience, maintain consistent incident reporting, and ensure that decision-makers understand the risks inherent in digital operations. As a consequence, governance responsibilities increasingly extend beyond IT departments and require active engagement from executive leadership.

Historically, IT governance and information security governance have evolved as parallel yet distinct areas: one concerned with performance, alignment, and value creation; the other with protecting the confidentiality, integrity, and availability of information. In practice, however, maintaining a strict separation between these domains can lead to inconsistent priorities, duplicated processes, and gaps that weaken organisational security. The interaction of technological and organisational factors supports the need for a more integrated approach.

The analysis focuses on the points at which IT governance and information security governance intersect and identifies areas where coordinated action enhances effectiveness. By analysing regulatory expectations, technological developments, and organisational needs, the paper outlines how integrated governance can support more coherent decision-making, more robust risk management, and improved operational resilience. The aim is to add to the existing discussion on governance development by presenting a framework that reflects the demands of today's digital environment and supports organisations in maintaining secure and reliable operations.

2 Research Methodology

The research presented in this paper is based on a qualitative analysis of current industry standards, regulatory documents, and academic literature. The methodology involved:

Literature Review: Examining existing frameworks such as COBIT 2019, ITIL 4, and ISO/IEC 27001 to identify overlapping control objectives and areas where strategic alignment is currently lacking.

Regulatory Analysis: A detailed analysis of the specific requirements of the NIS2 Directive and the Digital Operational Resilience Act (DORA) to determine their direct impact on corporate governance structures and executive accountability.

Synthesis and Model Proposal: Integrating the findings to propose a model where IT and security governance functions operate within a unified strategic framework, emphasizing shared data, common risk vocabularies, and joint reporting lines. The study focuses on the European context, as the EU's established standards often serve as a global benchmark for digital governance and resilience.

3 The Challenges of Cybersecurity Today

3.1 Growing Complexity of Cyberattacks and Threat

Ransomware and other forms of ransomware continue to evolve, with increasingly sophisticated attack techniques targeting critical infrastructure and business processes. [1] Using AI and machine learning enables attackers to quickly and automatically identify vulnerabilities, develop attack methods, and disguise themselves, thereby increasing the number of effective AI-based cyberattacks. [2] As attacks exploiting zero-day vulnerabilities pose a significant risk, effective and rapid vulnerability management is crucial. Data leaks and misuse of personal data remain a serious risk, with potentially severe reputational and financial consequences.

3.2 Regulation, Legislative Framework

Relevant information security regulations constantly evolve; companies must do everything possible to ensure compliance. New laws and increased data protection requirements can place additional administrative burdens on organizations and increase the risk of fines for non-compliance.

3.3 Safety at Work and Remote Working

Remote and hybrid working environments pose security challenges, as remote access to employee devices and company data opens up new attack surfaces. In addition to VPNs and multi-factor authentication (MFA), companies need to develop security solutions for remote work continuously.

3.4 Challenges arising from the technologies used

IoT (Internet of Things) security. With the proliferation of IoT devices, more and more potential attack surfaces are emerging, especially in smart homes, industrial systems, and the healthcare sector. These devices often have weak security defenses, making them easy targets for attackers. Central management and security updates for IoT devices can be challenging, especially if manufacturers do not provide regular device updates. [3] [4]

Cloud computing and cloud security. Companies increasingly turn to cloud services, but the shared responsibility model for data protection and security between cloud service providers is often unclear, leading to several security risks. API-based attacks and API security issues are also becoming increasingly important, as applications that use APIs are more vulnerable.

Artificial intelligence and machine learning in cybersecurity. Using AI and machine learning in cyber defense can enhance the protection of sensitive data and accelerate threat detection. At the same time, attackers can take advantage of these technologies to evade defenses. In addition, deepfake technology, which generates realistic but fake content, may be used in criminal activities such as identity theft or fraud. [5]

Cyberwar and geopolitical risks. Cyber warfare and political conflicts between nations could make cyberattacks even more prominent. Critical infrastructure, such as energy grids and health systems, could become targets of state-level attacks. [6]

Secure communication and privacy solutions. Encrypted communication and privacy solutions such as VPNs will continue to be essential. Governments' security, operation, and regulation of such systems can be a constantly evolving challenge.

4 Legislative responses to cybersecurity challenges in the EU – outlook

The main EU provisions and directives on information security aim to unify and strengthen Member States' information security regulation, enhance the protection of electronic information systems and their electronic data, and ensure compliance with the law. These provisions cover many sectors and areas, particularly the protection of personal data and the security of networks and information systems.

The main difference between directives and regulations:

- A directive is a legislative act that obliges Member States to achieve a specific objective through legislation under their responsibility. Member States have a margin of maneuver when transposing the directive.
- However, the Regulation is directly binding on all Member States and directly applicable throughout the EU, without the need for separate national legislation to implement it.

4.1 Electronic Communications Privacy - ePrivacy Directive, (2002/58/EC)

The ePrivacy Directive, often called the "cookie law," regulates the security and privacy of electronic communications. [7] It aims to protect data generated by online communications, including privacy in email, telephone, and other digital services. Key elements of the Directive include cookies and online tracking. The ePrivacy Directive requires that cookies be subject to authorization, meaning users must be actively asked to consent before cookies can be used. Another critical element is the security of electronic communications. The Directive ensures the confidentiality of data generated during electronic communications (e.g., call data and the content of messages). The ePrivacy Directive is currently being recast and is expected to be replaced by a new, stricter ePrivacy Regulation, more closely linked to the GDPR.

The first response to cybersecurity challenges was the creation of the European Network and Information Security Agency (ENISA) in March 2004.

This was followed in 2007 by a resolution on a strategy for a secure information society in Europe, highlighting that the challenges of the new phase of societal development are linked to ICT. [7] [8]

4.2 Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (CIP)

Directive 2008/114/EC established a regulatory framework for the protection of critical infrastructure in the European Union. The Directive provided a framework for identifying, designating, and protecting infrastructures while facilitating cooperation and cross-border coordination between Member States to ensure the security of critical systems and services. [9]

This was followed in 2009 by the publication of the "Critical Information Infrastructure Protection Action Plan," which has five main pillars: prevention and preparedness, detection and response, mitigation and recovery, international cooperation, and the definition of CIIs (Critical Information Infrastructure) in the ICT sector.

Communications from the European Commission and a Council position paper followed this. The Communication included the impact of the Internet on society and the requirement for trust and accountability in this regard. The resolution also highlighted the need for a high level of network and information security in the European Union and the importance of ICT and its security.

And in 2010, the Digital Agenda for Europe arrived. [10] The Agenda focused on seven key areas to boost the EU's global competitiveness in digital technologies. One of the seven pillars is strengthening cybersecurity and trust by increasing the security of digital systems and services.

In 2012, the fight against modern digital crime began with the creation of the European Cybercrime Center. [11]

The European Union's first cybersecurity strategy was published in 2013 under the title "An open, safe, and secure cyberspace." The aim was to make Europe a safe and secure digital space while preserving the openness and freedom of cyberspace. The strategy aimed to strengthen the EU's and its Member States' ability to defend against cyberattacks, enhance cyberspace security, and secure the EU's global position in cybersecurity. The strategy comprehensively addressed cyberspace threats and highlighted the importance of cooperation and accountability in improving cybersecurity. Its main pillars are improving cyber resilience, enhancing protection against crime, strengthening international cooperation in cyber defense, developing the cybersecurity industry, and raising awareness of cybersecurity threats.

4.3 PSD2 - Payment Services Directive (Directive 2015/2366/EU)

The PSD2 Directive regulates the security and transparency of digital financial transactions in the European Union. [12] Its main objective is to enhance the security of the financial sector and protect the rights of users of financial services through strong customer authentication and open banking.

In the context of Strong Customer Authentication (SCA), PSD2 requires strong customer authentication in financial transactions, which requires multi-factor authentication.

Under Open Banking, PSD2 opens up banks' APIs to third-party providers but requires strict security standards to protect data.

4.4 General Data Protection Regulation (GDPR) - Regulation (EU) 2016/679

The European Union's General Data Protection Regulation (GDPR) is the most essential piece of data protection legislation. [13] It aims to protect the personal data of natural persons and harmonize data protection rules in the Member States. The GDPR regulates the protection of personal data.

All data relating to natural persons is protected. The Regulation details the primary data processing principles (lawfulness, fairness, transparency, data minimization, etc.). It sets out the legal responsibilities of data controllers and processors, including data breach notification and compliance obligations. The GDPR can impose significant fines for non-compliance, up to €20 million or 4% of global annual turnover.

5 Legislative responses to cybersecurity challenges in the EU today

5.1 Cybersecurity Act, Regulation (EU) 2019/881

The EU Cybersecurity Act establishes a cybersecurity framework that sets out expectations for cybersecurity and provides a basis for cooperation between EU Member States. The role of the European Union Agency for Cybersecurity (ENISA) has been adjusted to support Member States in dealing with cyber threats. The Act establishes an EU-wide cybersecurity certification framework to help harmonize information security expectations across the European market. [14]

5.2 European Union Security Strategy 2020-2025

The European Union's Security Strategy 2020-2025 provides a comprehensive framework for the EU and its Member States to maintain internal security, address critical threats, and protect citizens. The strategy sets out measures intended to support safety and resilience within the EU, able to face evolving security challenges, including both traditional and digital threats. Its main messages are to create a timeless security environment by applying new security technologies, to address evolving threats and to prevent and detect threats in the online space, to build and maintain a robust EU security ecosystem by ensuring a solid security foundation, and to protect Europeans against terrorism and organized crime. The strategy focuses on threat prevention, rapid crisis response, and international cooperation. [15]

5.3 Critical Entities Resilience Directive (CER), Directive (EU) 2022/2557

The CER Directive (full name: Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical infrastructure organizations) is an essential piece of EU legislation that aims to enhance the resilience of critical infrastructure organizations, i.e., their ability to withstand various threats. [16]

Critical infrastructure: essential infrastructure necessary for performing basic social functions, health, safety, security, and economic and social well-being of people, the disruption or destruction of which has significant consequences. [17]

The CER Directive requires Member States to identify the most critical infrastructures and ensure appropriate security and protection measures are implemented, covering both cybersecurity and physical protection. Its main keywords are risk assessment, cooperation, authorities and SPOC, resilience measures, and human resource background checks. This legislation is an essential complement to the NIS2 Directive.

5.4 NIS 2 Directive - Network and Information Security Directive, (EU) 2022/2555

NIS2 is an essential step towards strengthening EU cybersecurity. [18] The NIS Directive (Network and Information Security Directive) aims to set uniform, high standards for cybersecurity. These organizations must implement and maintain specific security measures to protect their information systems against cyberattacks. The NIS Directive is the EU's first legal regulation on network and information systems security. It came into force in 2016 and aims to improve cooperation between Member States and increase the security of essential services. The Directive was replaced in 2023 by the NIS 2 Directive, which is even more widely applicable and sets stricter requirements. The NIS 2 Directive also introduces extended scope, risk management, and incident handling.

The harmonization of NIS 2 recognizes that cyberattacks are becoming more frequent and sophisticated, and that they seriously threaten Electronic Information Systems. It also addresses the lack of uniform regulation. The previous NIS Directive was insufficiently detailed and comprehensive, leading to significant differences in cybersecurity regulation across Member States. The NIS2 aims to remedy this situation and create a coherent regulatory framework.

Compliance with NIS2 is not only a legal obligation but can also be beneficial from a business perspective. Proper cybersecurity measures can protect your business from financial loss, reputational damage, and operational downtime. In addition, NIS2 compliance can also increase a company's competitiveness as customers and partners increasingly expect a high level of cybersecurity.

Detailed rules and requirements for NIS2 will be developed within the Member States' legal systems.

5.5 Digital Services Act (DSA), (EU) 2022/2065

The Digital Services Act aims to regulate the operations of online platforms, primarily social media and online marketplaces, to enhance online safety and protect users. [19] The main elements of the DSA include combating illegal content and protecting user data.

Platforms must have clear, transparent procedures for removing illegal content and protecting users' rights. The DSA will introduce tighter regulations to ensure user data security and increase online service providers' responsibility.

5.6 Digital Markets Act (DMA), (EU) 2022/1925

The Digital Markets Act aims to regulate competition on online platforms and digital markets to avoid abuses by big tech companies. Although it does not directly address information security, it is vital for enhancing the security of digital services and managing user data. [20]

5.7 DORA Regulation, Regulation (EU) 2022/2554

The Digital Operational Resilience Act (DORA) is also part of the European Union's information security legislation. [21] DORA applies specifically to the financial sector and aims to increase the digital operational resilience of financial institutions, particularly against cyber threats and other digital threats. DORA covers all financial sector actors, including banks, insurers, payment service providers, and critical third-party service providers. It aims to make the entire financial ecosystem resilient to cyber threats. The Regulation requires financial institutions to implement appropriate security measures to safeguard their digital operations, even in the face of significant disruptions (e.g., cyberattacks, technological failures). This is to maintain system resilience, manage cyber risks, and ensure continuity. Financial sector actors should regularly test the security and readiness of their Electronic Information Systems. In this context, DORA requires so-called penetration tests and other advanced security testing procedures. The regulation sets out requirements for the standards and guidelines that financial service providers must apply when managing cyber risks, including incident reporting. Improving incident management and rapid reporting to the competent authorities is an essential element. In particular, the Regulation sets out strict requirements for third-party technology service providers. The DORA is another critical part of the European information security regulations that will strengthen the protection and resilience of the financial sector's digital operations against cyberattacks and other technological disruptions.

6 The challenges of IT governance today

Information security governance provides the overarching framework for safeguarding the confidentiality, integrity, and availability of information. Within this framework, IT governance incorporates the necessary security controls to protect digital infrastructures, networks, and electronic information systems. The effectiveness of IT governance, therefore, presupposes a robust level of IT security, as the stability and reliability of technological environments directly shape the organisation’s operational resilience.

The expanding reliance on digital systems has considerably increased the strategic importance of IT governance. As organisations incorporate technology into core processes, the ability to maintain secure and dependable IT operations becomes a determining factor in organisational performance and continuity. At the same time, the proliferation of targeted cyberattacks underscores the need for governance arrangements that support informed decision-making and sustained risk management.

The challenges confronting IT governance arise from several structural and technological developments. A prominent factor is the accelerating pace of digital transformation, which compels organisations to adopt new platforms, service models, and architectural frameworks while preserving operational stability. The integration of IT into business processes requires regular coordination between technological and organisational leadership to ensure that IT-related decisions remain aligned with broader strategic objectives. [22]

Further difficulties stem from the relationship between business and IT functions. Divergent priorities, terminological differences, and distinct professional perspectives may hinder coordinated planning. Addressing these discrepancies calls for clearly delineated responsibilities and governance mechanisms that facilitate shared understanding and consistent oversight.

The shortage of skilled IT professionals presents an additional structural constraint. Rapid technological development necessitates continuous competence renewal, while many organisations face sustained pressure to secure and retain appropriately qualified personnel.

Modern IT environments are further characterised by growing technological complexity. Cloud-based and multi-provider infrastructures pose challenges in interoperability, access control, cost management, and defining responsibility boundaries between internal teams and external service providers. Ensuring consistent security measures and reliable service delivery within these environments requires governance structures capable of addressing these interdependencies.

Finally, the intensification of cybersecurity threats and the tightening of regulatory requirements place additional demands on IT governance. As electronic information systems become more interconnected, the organisational attack surface expands, and data protection requirements grow correspondingly more stringent. These developments increase the administrative and operational burden of compliance, particularly in incident reporting, risk assessment, and data governance. [23]

7 The challenges of information security governance today

Information security and traditional corporate governance share similar principles, aiming to achieve the organization's strategic objectives through governance and control mechanisms. While conventional corporate governance focuses on the management and control of the organization's overall business operations and the sustainable growth and management of the company as a whole, information security governance specifically addresses the protection of the organization's data assets and electronic information systems based on the principles of confidentiality, integrity, and availability (CIA). [24]

Electronic information security governance is a set of activities, processes, and rules for managing, organizing, and overseeing electronic information security to ensure that the protection of an organization's information assets is consistent with business objectives, regulatory requirements, and risk management principles. Information security governance provides a practical framework for the organization to manage and monitor processes related to information protection. This includes developing information security strategies, managing risk, overseeing and ensuring accountability, and complying with regulatory requirements.

Information security governance ensures that all levels of the organization understand the importance of information security and are involved in maintaining it. An organization can allocate resources more effectively by defining its information security objectives. Information security governance helps an organization comply with relevant legislation and standards (e.g., NIS2, GDPR, ISO27001), thereby enhancing the security and efficiency of business processes and reducing risks. Its main questions are who decides on information security issues, what principles and objectives guide these decisions, and how to ensure they are implemented. [25]

Information security governance is crucial to an organization's success, as it contributes to business continuity and competitiveness.

The biggest challenges to information security governance are posed by increasing technological complexity, emerging threats, and tightening regulatory expectations. Digital transformation, the rise of teleworking, and ever-changing data management and privacy expectations bring new challenges. Some of the main difficulties are outlined below:

Continuing growth and development of cyber threats. The number and sophistication of cybersecurity threats (e.g., ransomware, phishing, DDoS attacks) are increasing. New technologies, such as artificial intelligence and IoT (Internet of Things), create additional attack surfaces, so organizations must continually evolve their security strategy and tools. One of the significant challenges for information security governance is keeping up with threats and implementing effective risk management methods.

Changes in regulatory and compliance expectations. Regulations are becoming more complex and stringent, placing additional burdens on organizations to ensure information security. New

technologies are attracting additional regulatory attention, which may create new compliance requirements. The rapidly changing regulatory environment poses a significant challenge for organizations, as they must continuously adapt to these new requirements.

Compliance with regulations and data protection. Data protection is becoming an increasingly important issue worldwide. Organizations need to protect not only their business data but also their users' personal data, or face heavy fines if they do not comply with relevant laws. Compliance with data protection and security regulations is complex and requires constant attention.

The spread of teleworking and cloud services. Since the COVID-19 outbreak, more and more organizations have introduced telework, increasing security risks. Enterprises face the challenge of securing home and cloud-based devices, which are often less secure than corporate networks. Remote access to sensitive information requires more stringent security policies and technology solutions.

Complex technological environment. Modern organizations use more complex IT infrastructures and technologies, including cloud services, artificial intelligence, big data, and IoT. These new technologies significantly increase the complexity and surface of information security management attacks. The convergence of digitalization, IT, and business processes requires well-integrated security strategies that address gaps across systems.

Lack of security awareness. Information security is not only a technological issue but also a human factor. Lack of employee security awareness is one of the most significant risks. Social engineering and the exploitation of human error are standard attack methods. A key element of information security protection is providing appropriate training and security education to employees so they can respond to potential threats.

Budgetary constraints and lack of resources. Investing in information security can be expensive, and not all organizations have the financial resources to implement state-of-the-art security solutions. Securing an adequate IT security budget is challenging for many companies, especially when funding cybersecurity staff and tools.

Aligning IT and business goals. Aligning information security strategies with business objectives is often difficult. Implementing and maintaining IT security solutions can frequently slow down business processes, creating tensions between different parts of the organization. Lack of collaboration and communication between IT and business can also hinder effective information security management.

8 Synergies between information security governance and IT governance

IT governance and security governance fulfil distinct yet interdependent roles. IT governance, as reflected in frameworks such as COBIT and ITIL, establishes the organisational structures, processes, and decision-making mechanisms that guide IT services. Security governance, as defined by standards such as ISO/IEC 27014 and ISO/IEC 27001, establishes the security objectives, principles, and requirements that must inform these processes. Their relationship is reciprocal: IT governance provides the structural context for implementation, while security governance defines the protective requirements that IT systems and processes must incorporate.

The relationship between information security governance and IT governance is essential, as both aim to ensure the security, protection, and efficient operation of an organization's IT infrastructure. While the two domains remain distinct in scope, their interaction requires ongoing alignment to ensure that organisational, technological, and security objectives reinforce one another.

Information security governance focuses primarily on information protection. It aims to protect information from unauthorized access, modification, and destruction and to ensure its availability. IT governance has a broader scope and covers the entire life cycle of IT systems. It aims to ensure that electronic information and IT systems support business objectives while ensuring efficiency, availability, and security.

IT governance establishes the organisational and operational structures through which information security requirements are implemented, while the definition of those requirements belongs to security governance.

The distinction between the two concepts is important because they cover different areas and are the responsibility of other professionals. Information security governance is primarily the

responsibility of information security professionals, while IT governance is a shared responsibility of IT managers and business leaders.

However, they also have commonalities and synergies that can be harnessed to ensure more effective compliance and address today's challenges.

One of these is risk management. One of the core tasks of IT governance is identifying and managing electronic information system risks, including cybersecurity risks. Cybersecurity addresses specific threats and vulnerabilities related to IT infrastructure and data protection.

The link between Strategic Objectives and security objectives can also be exploited. The role of IT governance is to align IT strategies with the organization's business objectives. As part of this, information security strategies should also be designed to support business operations without hindering them. This includes implementing security controls that balance security with business agility.

Further synergies can be achieved by leveraging standard compliance and regulatory requirements. An important IT governance task is ensuring the organization complies with legal and regulatory requirements. Security governance provides the framework for translating compliance requirements into operational controls, reflecting the legal obligation to protect electronic information systems and the data they process. Security governance defines the security objectives and controls that IT processes and systems must incorporate.

Another area for action is control and supervision. Continuous monitoring and control of electronic information systems and processes are necessary for IT governance. The monitoring functions of cybersecurity systems ensure that potential threats are detected promptly and appropriate responses are taken quickly. In IT governance, these activities can be incorporated into formal control processes.

Synergies identified include incident management. For legislation resulting from NIS2 legal harmonization, "operational cybersecurity incident" and "cybersecurity incident" are already defined. [26] The former is a cybersecurity incident that unintentionally reduces or eliminates the availability of data stored, transmitted, or managed on electronic information systems or services offered or accessible through those systems. In contrast, a cybersecurity incident is defined as an event compromising the availability, integrity, or confidentiality of data stored, transmitted, or managed on electronic information systems or services offered by or accessible through those systems. Accordingly, IT and information security governance should work together to ensure the organization has appropriate incident management procedures in place.

In terms of resource management, one objective of IT governance is the efficient and cost-effective use of IT resources. From a security governance perspective, protective measures must be proportionate to the organisation’s risk exposure; security measures and their investment must be optimal, i.e., providing the proper protection while considering and using available resources where possible.

IT governance and cybersecurity are closely related, as both areas aim to ensure the effective operation and protection of an organization's IT systems. IT governance provides a broader framework for a strategic approach to cybersecurity, while cybersecurity supports achieving IT governance objectives through specific protection measures. An integrated cybersecurity approach is vital for companies to protect their assets and maintain business continuity.

8.1 Integration of IT and Security Objectives

The primary synergy between IT and security governance lies in the alignment of strategic goals. Traditionally, IT departments are measured by “uptime,” “speed of delivery,” and “user satisfaction,” while security teams are often perceived as functions that constrain delivery timelines. In organisational settings where cooperation between IT and security is well established, security is treated as an inherent element of IT service quality rather than an external control requirement. A system may meet functional requirements, yet without adequate security controls, its operational reliability remains limited. By aligning Key Performance Indicators (KPIs) with Key Risk Indicators (KRIs), organisations can ensure that IT investments are evaluated based on their total risk-adjusted value. For instance, when implementing a new ERP system, IT governance ensures it meets business needs, while security governance ensures the data it processes is protected. If these functions are synchronised, the resulting system is both functional and resilient, reducing the long-

term cost of remediation and breach-related losses. Such alignment supports organisational practices that incorporate security considerations early in system design and development.

8.2 Governance of Third-Party and Supply Chain Risks

One of the most critical areas of synergy is the management of the ICT supply chain. Modern enterprises are part of a vast ecosystem of cloud providers, software vendors, and managed service providers. As seen in significant supply chain incidents in recent years, a vulnerability in a single vendor can compromise thousands of clients. Integrated governance allows IT procurement and security risk management to work in tandem. IT governance provides the inventory and strategic rationale for vendor selection, while security governance performs the necessary due diligence and continuous monitoring. Under the DORA and NIS2 frameworks, regulatory requirements now make these measures explicitly mandatory. By merging these processes, organisations can shift from a minimal compliance-oriented assessment toward a model that evaluates suppliers based on their operational impact and associated risks. This involves not only reviewing a vendor’s certifications, but also understanding their role in critical business functions. In practice, unified vendor governance reduces the likelihood of oversight gaps that often arise when procurement and security reviews operate independently.

8.3 The Role of Leadership and Board Accountability

The most consequential alignment occurs at the organisational leadership level. Both IT and security governance require a clear and consistent commitment from senior management to be effective. The regulatory landscape of the mid-2020s (including NIS2 and DORA) explicitly places responsibility for cybersecurity risk management on the organisation’s management bodies. This means that board members can no longer delegate these responsibilities entirely to the CISO or CIO; they must actively oversee the risk-management framework. Synergistic governance supports this by providing the board with a consolidated overview of technology-related risks and operational dependencies. Instead of receiving separate, highly technical reports from IT and security units, the board is presented with a unified assessment of business-relevant digital risks. This supports more well-grounded decisions regarding budget allocation and strategic prioritisation. The explicit acknowledgement of IT as a core element of organisational risk management represents a significant shift in governance practice. When cybersecurity is treated as an integral part of corporate strategy, security initiatives receive appropriate support, and compliance obligations are met more consistently across the organisation.

9 Current Challenges and Regulatory Landscape

9.1 Technological Drivers

The transition to hybrid and multi-cloud environments has effectively dissolved the traditional network perimeter. Organizations can no longer rely on "castle-and-moat" security strategies; instead, they must adopt "Zero Trust" principles, in which every access request is continuously verified [27].

This shift requires a deep integration between identity management (an IT function) and threat detection (a security function). Furthermore, the emergence of AI as a tool for both attackers and defenders creates an arms race. While AI can automate patch management and anomaly detection, it also enables attackers to craft perfect phishing emails and discover zero-day vulnerabilities at scale [28].

9.2 Legislative Frameworks: NIS2 and DORA

The NIS2 Directive significantly broadens the definition of "essential" and "important" entities, bringing thousands of previously unregulated companies under strict oversight [18]. DORA, on the other hand, introduces specific requirements for the financial sector regarding digital operational resilience testing and third-party risk management [21]. These regulations move beyond technical checklists, focusing instead on the organization's ability to withstand, respond to, and recover from ICT-related disruptions. This holistic view of resilience is the cornerstone of modern governance.

Discussion

The analysis shows that the main obstacle to effective cooperation between IT governance and information security governance is organisational fragmentation, not technological capacity. Many institutions continue to operate with separate IT and security functions, each with its own objectives and resource allocations. This division leads to duplicated processes, inconsistent priorities, and gaps that can increase exposure to cyber threats.

Recent EU regulations—including NIS2 and DORA [13], [18], [21]—reinforce the expectation that organisations adopt more unified governance practices. These frameworks emphasise risk-based decision-making, clear accountability, and coordinated incident management, highlighting the limitations of siloed operational structures.

The analysis shows that an Integrated Governance, Risk, and Compliance (IGRC) model offers a structured approach to addressing these challenges. In such a framework, operational IT data (such as system logs and performance indicators) supports security monitoring activities. In contrast, threat and vulnerability information generated by the security function informs IT planning and patching cycles. This reciprocity creates a continuous feedback mechanism that supports a clearer operational picture and reduces the time required to respond to security events.

Organisational factors also remain significant. Skills shortages, uneven levels of security awareness, and unclear responsibility structures weaken the effectiveness of governance processes. Evidence supports the use of formalised roles, structured training programmes, and regular incident exercises to strengthen operational resilience [25]. Regulatory expectations concerning testing, incident reporting, and third-party oversight further encourage more systematic practices [18], [21].

The analysis shows that integrated governance strengthens organisational risk-management practices, improves resource prioritisation, and enhances operational continuity. In environments characterised by technological interdependence and increasing regulatory scrutiny, improved coordination between IT and information security governance has become essential to ensuring reliable, secure organisational operations.

Conclusion

The study demonstrates that aligning IT governance and information security governance has become increasingly important for organisations operating in complex digital environments. The combination of professionalised cybercrime, the emergence of AI-enabled attack techniques, and the heightened regulatory expectations introduced through instruments such as NIS2 and DORA creates conditions in which fragmented structures provide limited effectiveness. The evidence suggests that coordinated governance approaches provide clearer decision-making frameworks, reduce overlaps, and strengthen the organisation’s capacity to manage digital risks.

The synergies identified—strategic alignment, integrated oversight of technology and supply-chain dependencies, and defined governance responsibilities at the executive level—indicate that an integrated model contributes to greater consistency in risk management and operational planning. While its adoption may require adjustments to established organisational practices, particularly in the distribution of responsibilities and the coordination of processes, the benefits are measurable: enhanced resilience, more targeted resource allocation, and improved compliance with regulatory expectations.

As technology dependencies deepen and regulatory requirements expand, organisations that pursue integrated governance structures are better prepared to maintain continuity and to support secure development of digital services. Further research should examine how such models can be implemented in highly regulated sectors, where operational constraints and compliance obligations may shape the practical effectiveness of integrated governance and reveal additional opportunities for refinement.

References

[1] S. Duraibi, C. Kaur, and A. B. Pawar, “Cyber Extortion Unveiled: The Evolution, Tactics, Challenges, and Future of Ransomware,” in *2023 International Conference on Computational Science and Computational Intelligence (CSCI)*, 2023, pp. 861–867. doi: 10.1109/CSCI62032.2023.00144.

[2] S. Sur, M. El-Dosuky, and S. Kamel, “MACHINE LEARNING TECHNIQUES FOR CYBER SECURITY,” *J. Theor. Appl. Inf. Technol.*, vol. 102, no. 7, pp. 3002–3014, 2024.
[3] Gokhan Polat, “Security Issues in IoT: Challenges and Countermeasures,” ISACA. Accessed: Oct. 28, 2024. [Online]. Available: https://www.isaca.org/resources/isaca-journal/issues/2019/volume-1/security-issues-in-iot-challenges-and-countermeasures
[4] Larry G. Wlosinski, “The IoT as a Growing Threat to Organizations,” ISACA. Accessed: Oct. 28, 2024. [Online]. Available: https://www.isaca.org/resources/isaca-journal/issues/2019/volume-4/the-iot-as-a-growing-threat-to-organizations
[5] Y. Shang, “Detection and Prevention of Cyber Defense Attacks using Machine Learning Algorithms,” *Scalable Computing: Practice and Experience*, vol. 25, no. 2, Art. no. 2, Feb. 2024, doi: 10.12694/scpe.v25i2.2627.
[6] Y. Roumani and M. Alraee, “Examining the factors that impact the severity of cyberattacks on critical infrastructures,” *Computers & Security*, vol. 148, p. 104074, Jan. 2025, doi: 10.1016/j.cose.2024.104074.
[7] *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*, vol. 201. 2002. Accessed: Oct. 28, 2024. [Online]. Available: http://data.europa.eu/eli/dir/2002/58/oj/eng
[8] *Council Resolution of 22 March 2007 on a Strategy for a Secure Information Society in Europe*. 2007. Accessed: Feb. 11, 2025. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32007G0324(01)
[9] *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance)*, vol. 345. 2008. Accessed: Oct. 28, 2024. [Online]. Available: http://data.europa.eu/eli/dir/2008/114/oj/eng
[10] “COM_2010_245_616828_EN_ACTE_1_f_1.docx.” Accessed: Oct. 28, 2024. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52010DC0245
[11] “European Cybercrime Centre - EC3,” Europol. Accessed: Oct. 28, 2024. [Online]. Available: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
[12] *Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance)*, vol. 337. 2015. Accessed: Oct. 28, 2024. [Online]. Available: http://data.europa.eu/eli/dir/2015/2366/oj/eng
[13] *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) (Text with EEA relevance)*, vol. 119. 2016. Accessed: Oct. 28, 2024. [Online]. Available: http://data.europa.eu/eli/reg/2016/679/oj/eng
[14] *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) (Text with EEA relevance)*, vol. 151. 2019. Accessed: Oct. 28, 2024. [Online]. Available: http://data.europa.eu/eli/reg/2019/881/oj/eng
[15] “Internal Security Strategy (ISS) - EUR-Lex.” Accessed: Feb. 11, 2025. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum:internal_security_strategy
[16] *Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance)*, vol. 333. 2022. Accessed: Oct. 28, 2024. [Online]. Available: http://data.europa.eu/eli/dir/2022/2557/oj/eng
[17] “EU security union strategy | EUR-Lex.” Accessed: Oct. 28, 2024. [Online]. Available: https://eur-lex.europa.eu/EN/legal-content/summary/eu-security-union-strategy.html
[18] *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, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)*, vol. 333. 2022. Accessed: Oct. 28, 2024. [Online]. Available: http://data.europa.eu/eli/dir/2022/2555/oj/eng
[19] *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance)*, vol. 277. 2022. Accessed: Oct. 28, 2024. [Online]. Available: http://data.europa.eu/eli/reg/2022/2065/oj/eng
[20] *Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance)*, vol. 265. 2022. Accessed: Oct. 28, 2024. [Online]. Available: http://data.europa.eu/eli/reg/2022/1925/oj/eng
[21] *Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Text with EEA relevance)*, vol. 333. 2022. Accessed: Oct. 28, 2024. [Online]. Available: http://data.europa.eu/eli/reg/2022/2554/oj/eng
[22] A. Levstek, A. Pucihar, and T. Hovelja, “Towards an Adaptive Strategic IT Governance Model for SMEs,” *Journal of Theoretical and Applied Electronic Commerce Research*, vol. 17, no. 1, Art. no. 1, Mar. 2022, doi: 10.3390/jtaer17010012.
[23] A. Sbai, “Analysis of the Complexity and Risk to the Government eHealth System When Adopting the Cloud Services,” in *Innovative Technologies in Intelligent Systems and Industrial Applications*, S. C. Mukhopadhyay, S. M. N. A. Senanayake, and P. W. C. Prasad, Eds., Cham: Springer Nature Switzerland, 2024, pp. 181–200. doi: 10.1007/978-3-031-71773-4_12.

[24] X. Liang and Y. Xu, “A novel framework to identify cybersecurity challenges and opportunities for organizational digital transformation in the cloud,” *Computers & Security*, vol. 151, p. 104339, Apr. 2025, doi: 10.1016/j.cose.2025.104339.
[25] S. AlGhamdi, K. T. Win, and E. Vlahu-Gjorgievska, “Information security governance challenges and critical success factors: Systematic review,” *Computers & Security*, vol. 99, p. 102030, Dec. 2020, doi: 10.1016/j.cose.2020.102030.
[26] “Magyarország kiberbiztonságáról szóló törvénytervezet,” https://kormany.hu. Accessed: Oct. 28, 2024. [Online]. Available: https://kormany.hu/dokumentumtar/magyarorszag-kiberbiztonsagarol-szolo-torvenytervezet
[27] J. J. S. de Oliveira, “Zero Trust Architecture,” in *Cybersecurity: A Practitioner’s Guide*, 2023.
[28] S. J. Ghelani, “Cybersecurity in the Age of AI: Challenges and Opportunities,” *International Journal of Computer Trends and Technology*, vol. 70, no. 10, pp. 24–28, Oct. 2022.