Architecture
Image Studies

Vol.7, Issue 1, pp.2602-2621, 2026
DOI: https://doi.org/10.62754/ais.v7i1.1285

https://journals.ap2.pt/index.php/ais/index

# From Compliance to Cyber Resilience:Bridging Governance Gaps in Regulatory Cybersecurity Frameworks

## A Critical Analysis of Regulatory Evolution and Organizational Adaptation.

Yasir Majeed[1], Anas Majeed[2]

### Abstract

The growth of regulatory cybersecurity systems across the globe has led to the development of a compliance-focused paradigm that, amid defining minimum security standards, frequently tends to overlook the adaptive, agile skills required of organisations to be cyber resilient. This paper will critically review the governance failures of compliance-based methods in cybersecurity and a new system of integrated governance that can accommodate both classic regulatory compliance and the principles of cyber resilience. With the assistance of a comparative analysis of the leading regulatory frameworks such as NIST CSF, ISO 27001, GDPR, NIS2 Directive, and DORA, and the analysis of high-profile cybersecurity incidents, we single out the systematic shortcomings in governance: checklist mentality, insufficient incident recovery procedures, ineffective accountability frameworks, and the lack of adaptive governance capabilities. The Cyber Resilience Governance Model we propose integrates compliance need with resilience concepts in four combined layers of governance, namely strategic, operational, and tactical and oversight with supporting continuous improvement mechanisms and cross-functional accountability frameworks. The framework fills in some critical gaps like adaptive risk management, organisational learning of incidents, supply chain resilience and human factors integration. The study is relevant to the body of research on cybersecurity governance in the sense that it offers both theoretical and practicable advice to policy makers, regulators, and organisational leaders who are in need of shifting their focus on reactive compliance to proactive resilience. These results are relevant to the corporate governance practices, regulatory design, and operationalisation of the cyber resilience of critical infrastructure areas.

**Keywords:** *Cyber Resilience, Cybersecurity Governance, Regulatory Compliance, Risk Management, Organisational Resilience, Governance Frameworks, Critical Infrastructure, Incident Response.*

## Introduction

The world cybersecurity environment has changed significantly in the last ten years with a dramatic growth in the rates of cyber-attacks, as well as their frequency and complexity. Based on the economic consequences of cybercrime, it is estimated that the risk will increase to $10.5 trillion every year by 2025, and the impact of attacks on critical infrastructure has already shown how failures in any system can spread across the connections (Lone et al., 2023; Thakur & Pathan, 2020). This changing environment of threats has triggered a regulatory reaction of unprecedented scale and intensity, as governments and regulatory agencies the world over have introduced obligatory cybersecurity regimes in sectors such as financial services to healthcare and critical national infrastructures (Dupont, 2012; Sulich et al., 2021).

The dominating regulatory model has been mainly aimed at instituting compliance-based models that require baseline security controls, reporting requirements, and governance model(Zarrabi Jorshari, 2016). An example of this compliance-oriented paradigm is frameworks like the General Data Protection Regulation (GDPR), the Network and Information Systems Directive 2 (NIS2) the Digital Operational Resilience Act (DORA) and many versions of the NIST Cybersecurity Framework. Although these frameworks have certainly brought the standard of cybersecurity to a new level and established

[1] The University of Lahore, Email: yasirmajeedsatti@gmail.com, (Corresponding Author)
[2] Victoria University Melbourne, Australia, Email: anssatti7@gmail.com

mechanisms of accountability, there is an emerging body of evidence that indicates that there is a fundamental disconnect between the attainment of compliance and the real capability of resiliency(Loumachi et al., 2025).

**The Compliance-Resilience Paradox**

An in-depth analysis of the high-profile cybersecurity cases shows a problematic trend: organisations that passed the regulatory compliance tests often demonstrated a severe vulnerability under the pressure of complex attacks or systemic disruption (Zamil & Faruq, 2022). The 2021 Colonial Pipeline ransomware attack, the 2021 Solar Winds supply chain breach and the numerous times the healthcare sector has had organisations with ISO 27001 certification being breached demonstrate the fact that compliance documentation may not always equate to operational resilience(Mehmood et al., 2025). This disjuncture - which we refer to as the compliance-resilience paradox - is indicative of inherent constraints regarding the manner in which the present regulatory frameworks are conceptualizing, measuring, and incentivising cybersecurity capability. These factors must be considered in the implementation of this approach (National Cyber Security Centre, 2022; U.S. Department of Homeland Security, 2023).

The compliance-resilience paradox occurs at different planes. The compliance models generally focus on end of period evaluations, record keeping of controls, and compliance with recommended standards- developing the mentality of a check box that meets the audit test yet may ignore the dynamic, flexible capabilities that a robust organisation needs. Moreover, compliance frameworks are usually more concerned with prevention and detection, but little is said about response, recovery and organisational learning processes that create the difference between resilient systems and not just compliant systems (Qudus, 2025).

**Research Objectives and Questions**

The paper is based on the following main research question: How can cybersecurity governance and frameworks help to effectively address the gap between the requirements and organisational capabilities of cyber resilience in regulatory compliance? This general question is answered using four research questions:

What are the fundamental governance gaps in current compliance-driven cybersecurity frameworks that impede the development of cyber resilience?

How do major regulatory frameworks differ in their approach to resilience, and what insights can comparative analysis yield for future regulatory design?

What governance mechanisms, structures, and processes are required to operationalise cyber resilience within organisations subject to regulatory requirements?

What integrated governance model can effectively synthesise compliance obligations with resilience principles whilst addressing identified governance gaps?

**Conceptual Foundations**

This section forms the theoretical background that is needed to comprehend the interrelationship between regulatory compliance and cyber resilience. We analyse four interrelated areas of conceptualisation compliance-focused models of cybersecurity, cyber resilience differentiated out of traditional cybersecurity, governance and regulatory theory, and organisational resilience frameworks.

**Compliance-Driven Cybersecurity Models**

Compliance-based cybersecurity is a regulatory strategy where organisations deploy security controls, procedures and governance frameworks with the main purpose of meeting externally imposed requirements as opposed to meeting contextually relevant risks (Singh, 2025a). The development of this paradigm was based on technical regulatory paradigms used in areas like financial auditing, environmental protection, and occupational health and safety using a version based on the perceived necessity of minimum cybersecurity standards across industries and jurisdiction (Obioha-Val, 2025).

There are a number of features that define the compliance model. First, it sets prescriptive standards which outline specific controls or practices that organisations should undertake and this sets up standardised minimum levels that are supposed to achieve minimum security(Kala, 2024). Second, it has assessment and certification mechanisms: audits, certifications, attestations which give an external confirmation of compliance status. Third, it generally contains enforcement measures,

penalties, sanctions, regulatory measures that establish incentives to obey. Fourth, it has a focus on documentation and evidence, which has organisations prove compliance by policy, procedure, and records (Sharma et al., 2023).

Scholarly sources on compliance-based strategies have found advantages as well as drawbacks. Such advantages as standardisation allowing comparison and assessment across organisations, the development of minimum security baselines that improve the practice in particular among laggard organisations, provision of a set of clear accountability with defined roles and responsibilities, and creation of clearer structures reducing uncertainty surrounding security requirements are brought about (Hossain et al., 2022). Nevertheless, experts have started to find the weaknesses: the propensity to checkbox compliance where organisations address letter and not spirit of requirements; a lack of dynamic to organisation-specific contexts and risk profiles; the focus on one-time, point-in-time evaluations as opposed to continuous improvement; and the possibility of crowding out innovation and context-appropriate security investments (Melaku, 2023a).

**Cyber Resilience: Conceptual Distinctions**

Cyber resilience denotes a paradigm shift in thinking as compared to traditional cybersecurity, yet the two terms have been confused in reality. Unlike conventional cybersecurity, which mostly focuses on prevention and protection, i.e., keeping the adversaries outside the organization and ensuring that the systems stay intact, cyber resilience recognizes that successful attacks and compromises of the systems are inescapable and focuses on the ability to foresee, resist, recover, and adapt to the negative cyber incidents (Melaku, 2023b; Shrestha, 2025).

According to the National Institute of Standards and Technology, cyber resilience refers to the capacity to foresee, endure, recuperate, and modify the adverse state, load, assaults, or infiltration of the systems that employ or empower cyber assets (Faruq & Mollah, 2021). In this definition four fundamental capacities are involved. Anticipation entails proactive threat intelligence, scenario planning, and risk assessment that helps organisations to realise potential threats before they occur. The ability to keep critical functions intact in the face of attacks due to redundancy, segmentation and continuity is referred to as withstanding. Recovery refers to the capability to recover normal operations efficiently and promptly after incidences. Adaptation entails incident-based learning and development of counter measures to resolve arising threats and vulnerabilities (Oh et al., 2025a; Young, 2025a).

**Regulatory Cybersecurity Framework Landscape**

The international cybersecurity regulatory environment has become a complicated network of frameworks, standards, and requirements that all differ in the scope of the area, strategy, and implementation systems (Anil & Babatope, 2024a). This section compares key frameworks, their implications on governance, implementation issues and their method of treating resilience.

**NIST Cybersecurity Framework**

The NIST Cybersecurity Framework (CSF), which was first published in 2014 and most recently in 2024 (version 2.0), is a voluntary and risk-based framework to assist organisations in dealing with cybersecurity risks. In a reaction to the Executive Order 13636 because of the need to protect critical infrastructure, the framework has six main functions in which the cybersecurity operations are organised: Govern, Identify, Protect, Detect, Respond, and Recover (White & Sjelin, 2022). The NIST CSF implications of governance revolve around its voluntariness and flexibility of application (Möller, 2023). Although in practice, it is not required by law in most organisations, it has become the de facto standard especially in the critical infrastructure sectors and supply chain demands. The model clearly touches on the issue of resilience using its Respond and Recover functions, which focus on incident response, recovery planning and the process of improvement (Alshar'e, 2023; Calder, 2018).

**ISO/IEC 27001 and 27002**

The ISO/IEC 27000 family is an international standard of an information security management system (ISMS) and ISO 27001 is a standard outlining requirements to establish, implement, maintain, and continuously improve an information security management system (ISMS), and ISO 27002 is a standard that provides a detailed guideline on security control. The standard is focused on a process-oriented strategy that focuses on risk assessment, risk treatment and continuous improvement of risk treatment using Plan-Do-Check-Act loops(Calder, 2020; Disterer, 2013).

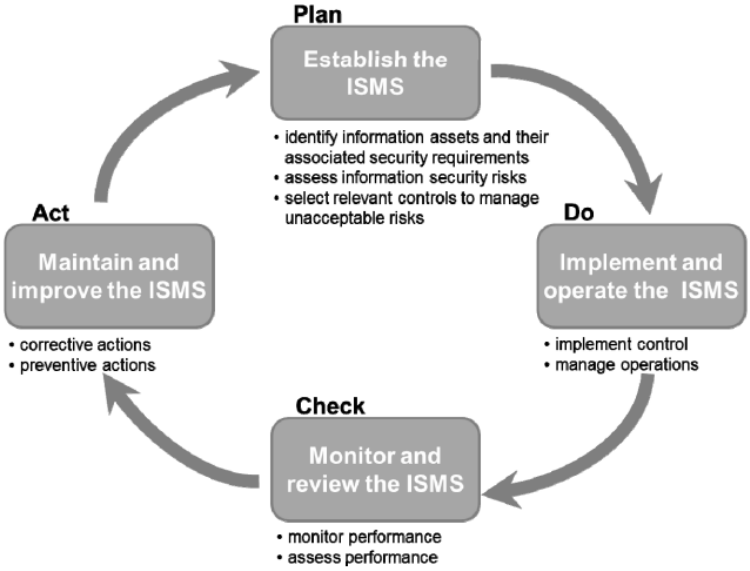


**Figure 1: PDCA cycle in ISO 27000. (ISO 27000, 2009)**

The figure 1, shows the Plan-Do-Check-Act (PDCA) cycle employed in ISO/IEC 27001 to build and continually enhance an Information Security Management System (ISMS), and ISO/IEC 27002 is a more practical approach to the selection and application of controls. During the Plan phase organization will identify information assets, evaluate risks, and select suitable security measures, during Do, these measures should be put into action and operated, during Check, monitoring and evaluation of performance and effectiveness of the information security measures must be observed and finally under Act corrective and preventive actions must be undertaken to improve the ISMS so that the information security practices continuously improve.

Governance implications consist of the standard requirements on commitment of the top management, security policies, role and responsibility definition, and management review. Accountability is developed by the certification process, as it entails third party audits. But critics claim that the control-focused nature of the standard is thorough but that it can focus on documentation and compliance, rather than on effective security and resiliency, in practice(Alrehili & Alhazmi, 2024).

**NIS2 Directive and DORA**

In 2022, the Network and Information Systems Directive (NIS2) was revised, adding to the range of actions in the field of cybersecurity regulation in the EU on a larger scale (Clausmeier, 2023). NIS2 expands sectoral and organisational requirements, reinforces security requirements, harmonises enforcement and presents clear-cut supply chain and incident notification requirements (Vandezande, 2024). In contrast to its predecessor, NIS2 increases the responsibility of management bodies since it explicitly states that they must approve cybersecurity risk management measures and control implementation (Ivaščevs et al., 2025).

DORA (Digital Operational Resilience Act), which will become effective in January 2025, creates a broad framework of digital operational resilience in particular to the EU financial sector. DORA is unique in terms of explicitly focusing on resilience as opposed to security or compliance, ICT risk management, incident reporting, resilience testing of operations, third-party risk management, and sharing of information (Boddy, 2024). Under the regulation, management bodies are expected to have a final accountability in the management of ICT risks and within it, a number of governance arrangements are required such as definition of roles and responsibilities, sufficient allocation of resources, and periodic reporting to the management (Espinoza et al., 2023).

**Table 1: Comparative Regulatory Framework Analysis**

| Framework | Scope | Approach | Resilience Focus | Key Governance Requirements |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| **NIST CSF 2.0** | Cross-sector, critical infrastructure | Principles-based, risk-focused | High—explicit Respond/Recover functions | Govern function; risk management; continuous improvement |
| **ISO 27001:2022** | International, all sectors | Process-based ISMS | Moderate—business continuity controls | Top management commitment; PDCA cycles; management review |
| **NIS2 Directive** | EU essential/important entities | Risk management and resilience | High—explicit resilience requirements | Management oversight; supply chain; incident notification |
| **DORA** | EU financial sector | Comprehensive operational resilience | Very High—centred on resilience | ICT risk management; resilience testing; third-party oversight |
| **GDPR** | EU/EEA personal data | Principles-based with specific requirements | Low—data protection focus | Accountability; DPO requirements; breach notification; DPIA |

The table 1, gives a comparative existence of key cybersecurity and data governance frameworks by analysing their scope, regulatory approach, resilience orientation, and governance requirements. NIST CSF 2.0 cuts across the industries, particularly critical infrastructure utilizing a principles-based, risk-oriented strategy with robust resilience elements and explicit response and recovery functions, along with requirements of governance, risk management, and continuous improvement. Internationally applicable industry-wise, the ISO 27001:2022 standard uses a systematic Information Security Management System (ISMS) by placing moderate focus on resilience largely through business continuity controls, along with strong management commitment and cycles of improvement. The NIS2 Directive is focused on fundamental and valuable EU bodies and ensures risk management and resilience responsibilities, such as supply chain security and incident reporting that have direct management. Specialized in the EU financial sphere, DORA puts the most emphasis on operational resilience, requiring ICT risk management, resilience testing, and control over the third-party service providers. Contrary to this, GDPR basically deals with personal data protection in the EU/EEA with little resilience thought, and focuses on accountability, data protection governance, breach notification, and impact assessment. On the whole, the comparison reveals that there is a way to data protection frameworks to more resiliency-focused cybersecurity governance frameworks.

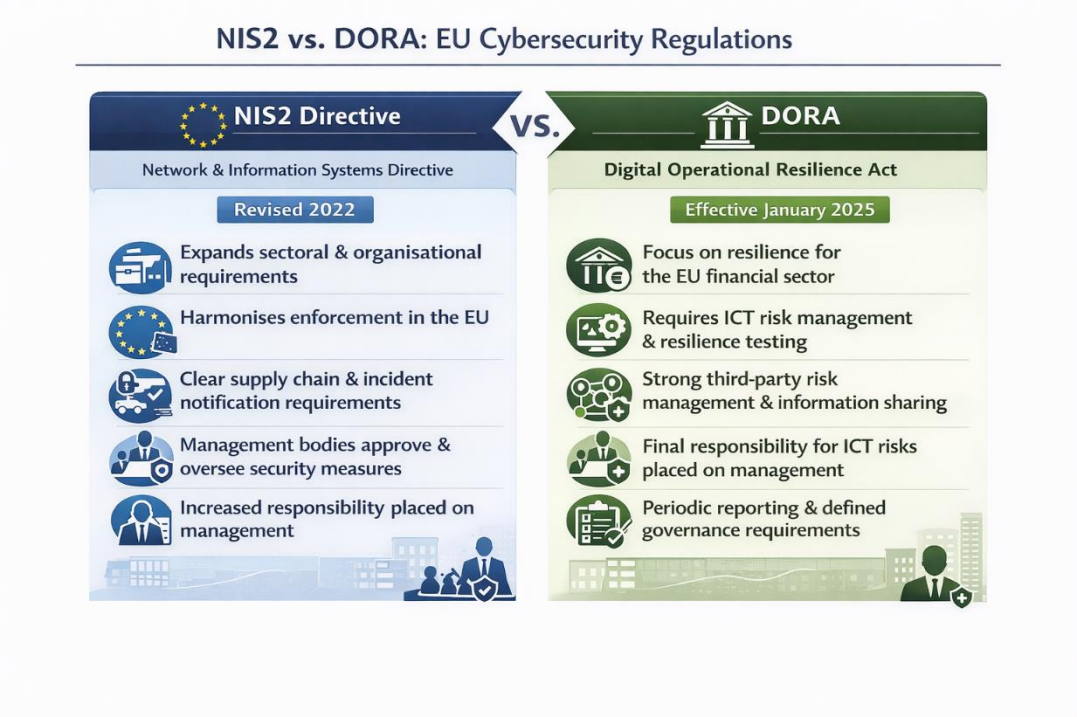


**Figure 2: NIS2 Vs. DORA: EU Cybersecurity Regulations**

The figure 2, is a comparison of the two significant cybersecurity regulations the EU has issued, namely, NIS2 and DORA, in terms of scope, priorities, and the implications of their governance. The revised NIS2 (2022), is more comprehensive in cycling cybersecurity requirements through most sectors, aligns enforcement of cybersecurity across EU member states, refines supply chain and incident reporting responsibilities, and substantially increased management responsibility by obligating leaders to affirm and monitor cybersecurity risk management. Conversely, DORA, which is effective as of January 2025, focuses particularly on the EU financial sector and is based on the idea of digital operational resilience, which extends beyond most traditional security compliance. It requires ICT risk management, resilience testing, incident reporting, third-party risk management and information sharing and lays ultimate responsibility on the management bodies concerning ICT risks through proper governance structure, defined roles, sufficient resources and frequent reporting. Collectively, the illustration indicates that as much as NIS2 introduces more extensive governance of cybersecurity, DORA offers a more detailed framework of resilience-related regulation of financial institutions

## Governance Gaps in Compliance-Driven Security

Regardless of the spread of regulatory cybersecurity frameworks and the growing organisational commitment to compliance efforts, it is still evident that there are large governance gaps, which compromise the creation of true cyber resilience (Folorunso et al., 2024). This section analyses these gaps in a systematic manner by exploring how compliance-based strategy generates structural weaknesses that expose organisations as vulnerable in spite of seemingly complying with regulation.

### Checklist Compliance Mentality

The most widespread governance gap manifests through what scholars describe by the term checklist compliance that is the propensity to turn cybersecurity into a set of discrete and auditable controls that can be implemented, documented and certified without the development of built-in resiliency capabilities (Akinsola, 2025). The phenomenon is the rational organisational reactions to the regulatory incentives: documentation of compliance offers the defensible evidence of due diligence, meets auditors and protects organisations against liability. The compliance mentality gives rise to what Power (2007) refers to as organised hypocrisy the presence of formal structures and processes, which symbolically reflect compliance but do not actually fulfil security goals (Gómez et al., 2025). The governance gap has a number of instances. The compliance activities lose the touch with the risk management and the security teams are focused on the needs of the auditors instead of the real threat (Omolere, 2025). The prioritisation of investments give more importance to controls that satisfy

compliance appropriations rather than those that mitigate risks which are specific to the organisation (Popoola & Ibrahim, 2024).

**Inadequate Operational Resilience Focus**

The majority of regulatory frameworks tend to prioritize prevention and protection, keeping enemies out, ensuring data confidentiality and integrity, and keeping unauthorised access to a minimum (Lichte et al., 2022). Although these goals are critical, the sole emphasis on prevention makes prevention leave a gap in governance concerning the ability to respond, recover, and adapt to the situation. Organisations can have high compliance rating of preventive controls and still have poor incident response, lack of backup and recovery system, or even no business continuity plan in case of cyber incident (Ositashvili, 2024). The gap in operational resilience is in the form of various critical gaps. Incident response plans are there to meet compliance needs but are not tested, which creates a false sense of security that vanishes in case of incidents. Business continuity planning considers cyber incidences as secondary to the conventional disaster planning. Compliance recovery time objectives and recovery point objectives are set, but not tested (Buttigieg & Zimmermann, 2024).

**Fragmented Accountability Structures**

Cybersecurity roles are usually defined in compliance frameworks at the IT or security functions forming organisational silos that hinder overall resiliency. The fragmentation is vertical and horizontal, which is not enough board engagement and executive accountability and the coordination between business functions, IT, risk management, legal and operational units (Singh, 2025b). The governance at the board level is highly lacking even in organisations that claim to comply with the requirements of governance (Heim, 2023). Board members are often not cybersecurity experts to offer valuable oversight, delegate to technical experts without challenging the strategy, get compliance-oriented reporting that masks risk exposure and do not have consistent supervision but only engage intermittently (Agarwal & Shah, 2024; Azmi et al., 2018; Fan, 2024). Horizontal fragmentation brings about coordination failure. The security teams cannot see or have control over business processes and technology decisions that pose risks.

**Weak Incident Learning Mechanisms**

Security incident organisational learning is a crucial resilience ability, although compliance systems fail to accommodate learning processes poorly. Although most of these frameworks mandate that the incident should be reported to the regulators, they do not force or encourage the systematic analysis and learning and improvement that ought to be conducted after the occurrence of the incident (Ahmad et al., 2020; Taylor et al., 2021). Post-incident reviews sometimes by organisations often focus on what caused the incident, including immediate technical factors, such as the vulnerability that was exploited, the credential that was compromised, but usually not on the deeper governance failures, systemic failures, or strategic consequences (Rezazade Mehrizi et al., 2022). Learning gap works on various levels. Technically, organisations can fix individual vulnerabilities without responding to larger trends of security debt or architectural vulnerabilities. On the operational level, they can be able to change certain processes without looking into the root process failures and capacity limitations (Huber et al., 2009). Through the governance level, they hardly challenge strategic assumptions, resource allocation choices, and organisational structures which facilitated incidents.

**Table 2: Governance Gap Matrix**

| Governance Gap | Compliance Manifestation | Resilience Requirement | Governance Mechanism |
|---|---|---|---|
| **Checklist Compliance** | Controls for audit success; disconnected from risk | Context-aware, risk-based security | Integrated risk governance; effectiveness metrics |
| **Prevention Bias** | Overemphasis on prevention; inadequate response/recovery | Rapid detection, effective containment, swift recovery | Incident response governance; business continuity; resilience testing |
| **Fragmented Accountability** | Siloed security function; weak board engagement | Clear ownership; cross-functional collaboration | Three lines model; cyber risk committee; RACI matrices |

| | | | |
|---|---|---|---|
| **Static Governance** | Fixed policies; slow adaptation | Dynamic threat-informed security; adaptive capacity | Threat intelligence integration; continuous improvement |
| **Weak Learning** | Superficial incident reviews; repeated mistakes | Systematic learning; root cause analysis | Post-incident review process; lessons learned repository |

The Governance Gap Matrix in table 2, identifies the generic vulnerabilities in organizational cybersecurity governance and compares them to the resiliency that is possible to mitigate the vulnerability, and indicates how such vulnerabilities can be remedied. Most organizations have a checklist compliance whereby controls are established with the primary aim of meeting the audit process, as opposed to focusing on the actual risks; resilience demands context-based, risk-based security enabled through integrated risk governance and performance metrics. An insufficient preparation of incident response and recovery is often caused by a prevention bias, and resilient systems are prepared to quickly detect, contain, and recover through incident response governance and resilience testing. Divided responsibility leads to siloed security operations and lack of leadership involvement whereas resilience needs to be defined ownership and cross-functional integration using governance frameworks such as cyber risk committees and responsibility frameworks. Fixed governance structures find it difficult to respond in line with changing threats and therefore constant improvement and integration of threat intelligence is critical to resilience. Lastly, the presence of weak organizational learning whereby analysis of incidents is done poorly and repetitive errors made should be substituted with systematic post-incidents reviews and institutional learning processes. Generally, this table demonstrates that resilience demands adaptive, coordinated, and continuously learning governance systems, as opposed to compliance-driven and reactive ones.

**From Compliance to Cyber Resilience: Transition Mechanisms**

This model shows the four levels of organizational cybersecurity maturity in four quadrants. Q2 with the red border is the so-called compliance gap wherein organizations obtain high compliance scores and low resilience capabilities, which is the core of the current study. The blue arrow shows how much it has to shift the governance to Q4 which is the desired state of integrated governance between high compliance and high resilience.

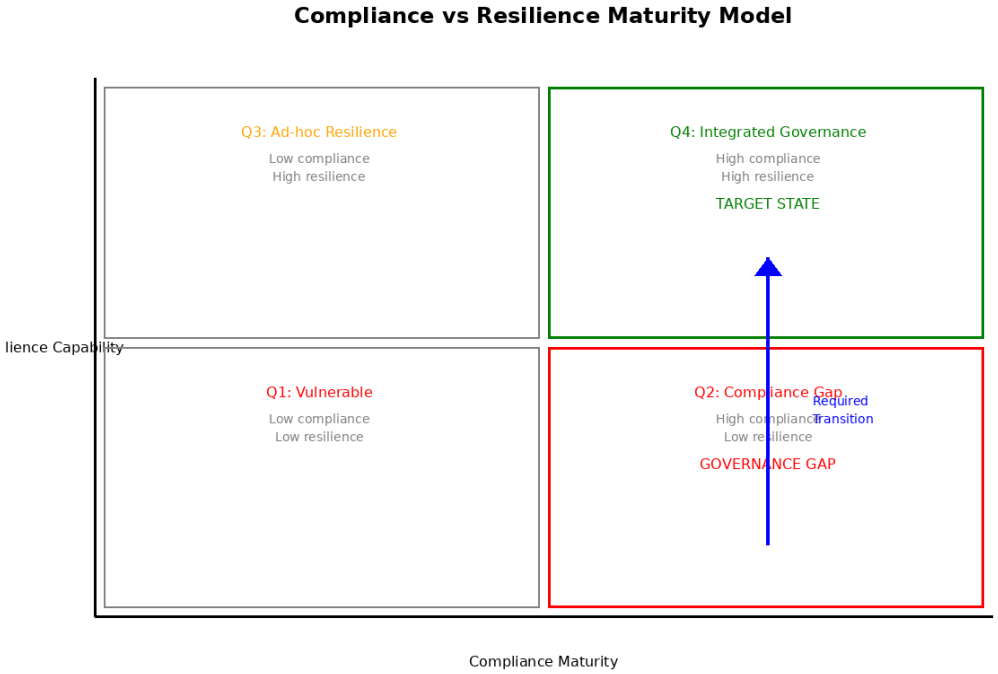


**Figure 2: Compliance vs Resilience Maturity Model**

The figure 2, provides a Compliance vs. Resilience Maturity Model that depicts the maturity of organizations in two dimensions, as compliance maturity (horizontal axis) and resilience capability

(vertical axis). Low compliance and weak resilience is the condition of organizations in Q1 (Vulnerable), which exposes them to operational and cyber risks. Q2 (Compliance Gap) are those organizations that have attained regulatory compliance but are operationally fragile, posing a gap in governance in which controls are present but recovery and adaptive capabilities are very weak. Q3 (Ad-hoc/Reactive Resilience) includes those organizations which demonstrate high resilience practices, yet have inadequate formal compliance systems. The Q4 (Integrated Governance) desired state is the one with high compliance, and high resilience, where governance, risk management, and operational practices are completely integrated so that organizations can respond to, overcome, and recover, as well as meet regulatory requirements, in this way. The arrow of upward transition shows the strategic necessity to shift to integrated governance which is resilience-oriented rather than compliance-oriented.

The given model is consistent with the literature on resilience governance that states that organizations should not rely on compliance-based security but, instead, develop adaptive, risk-aware resilience competencies to effectively handle contemporary systemic risks (Carías et al., 2020; Zighan, 2024). A shift toward real cyber resilience over compliance-based cybersecurity necessitates a major shift in organisational governance, culture, capabilities, and measurement strategies. This shift cannot be described only as additive, i.e. the introduction of resilience capabilities and compliance activities that are already in place, but transformative that demands the redefinition of cybersecurity as a strategic organisational ability, but not as a regulatory imposition (Pemmasani, 2023).

**Adaptive Risk Management**

The core competency to cyber resilience is adaptive risk management, where the current, dynamic, threat-driven risk management replaces passive, sporadic risk analysis. This necessitates the incorporation of threat intelligence and vulnerability management, asset criticality analysis and business impact analysis into an integrated set that is used to make real-time decisions instead of relying on an annual compliance cycle (Itani et al., 2024). Adaptive risk management involves some important components to implement. Organisations need to have a continuous monitoring ability that offers insights into their security posture, threat landscape and control efficacy (Sabidi & Zolkipli, 2024; Young, 2025b). They need to build threat intelligence that will guide risk determination with the existing threat actor tactics, techniques and processes. They will have to develop risk quantification procedures that will enable them to convert the technical vulnerabilities and threats into the business impact measures (Aghazadeh Ardebili et al., 2024; Bahmanova & Lace, 2026).

**Organisational Resilience Integration**

Cyber resilience is not possible without the inclusion of technical security but must be incorporated with more organisational resilience capacity (Bima & Intan, 2024). This integration acknowledges the fact that cyber incidents carry business implications such as disruption of operations, financial losses, reputational losses, regulatory fines which are not limited to IT systems (Novokreshchenova, 2025). The mechanisms to integrate involve joint scenario planning and testing, which is conducted in both technical and business terms, unified governing structures which encompass cybersecurity and operational risk and business continuity leaders, integrated crisis management processes, and standardized metrics and reporting structures which allow assessment of resilience in a holistic form (Rajola et al., 2025).

**Continuous Resilience Validation**

One of the main differences between compliance and resilience can be seen in the validation. Compliance may be illustrated by documentation and audits at a point in time. On the other hand, resilience must be constantly tested under what can be considered real-life conditions, and its ability to withstand pressure made in stressful situations. Some validation methods are technical resilience testing, tabletop exercises, crisis simulation exercises, red team assessments, and supply chain resilience testing (Uddoh et al., 2021). These type of validation activities are not only useful in proving compliance. They find holes in plans, procedures and capabilities; they establish organisational muscle memory of crisis response; they expose dependence and single points of failure; they authenticate communication protocols and decision-making processes and evidence of continuous improvement (Choi et al., 2023; Conklin & Shoemaker, 2017).

**Proposed Cyber Resilience Governance Framework**

This section provides an integrated Cyber Resilience Governance Framework based on the governance gaps analysis and needs at the transition that synthesises compliance requirements and resilience principles. The framework works at four governance levels, including Strategic, Operational,

Tactical and Oversight, and each has specific roles, processes and integration mechanisms(Melaku, 2023c). The resiliency life cycle consists of six phases related to each other in the form of a constantly improving cycle. This model focuses equally on response, recovery, and adaptation as opposed to the traditional compliance methods that have placed more emphasis on prevention and detection(Anil & Babatope, 2024b). The main cycle of Continuous Improvement is an indicator of the perpetual character of resilience governance(Christine & Thinyane, 2022). Gray arrows reveal the cycling movement among stages, whereas the governance integration locations on the bottom denote how the board oversight, metrics, cross-functional coordination, and regulatory compliance are integrated all over the cycle instead of being separate activities.

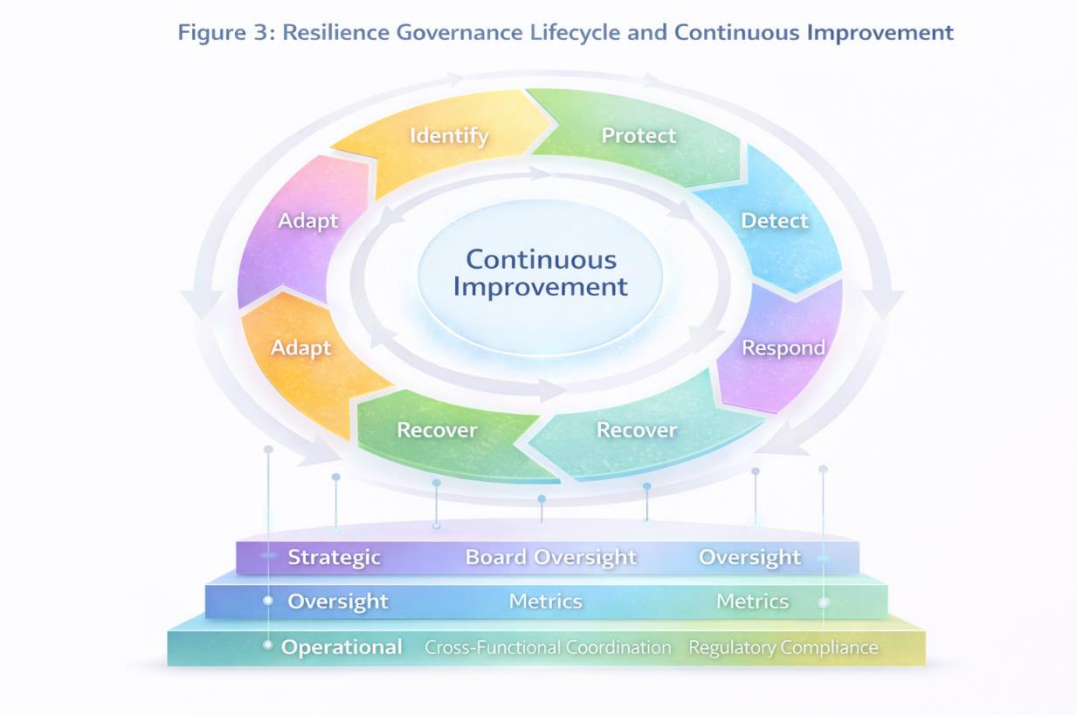


**Figure 3: Resilience Governance Lifecycle and Continuous Improvement**

The figure 3, depicts the Resilience Governance Lifecycle and Continuous Improvement model, which states how organizational resilience is worked out in the model of a constantly developing governance and operational cycle. The lifecycle passes through six phases that are interrelated and directed towards ensuring that the institutions do not only avoid and detect disruptions but also respond, recover, and keep adapting to the new risks, namely, Identify, Protect, Detect, Respond, Recover, and Adapt. Under Continuous Improvement, which is in the centre, it is stressed that resilience is not a first-time event but a process that is sustained through lessons gained and performance appraisal. Layered governance functions and multiple levels of operation support this lifecycle including strategic leadership and board control, performance measurements and monitoring, cross-functional operation coordination and regulatory compliance function which are integrated during the cycle and not independent. The arrows on the circle show the adaptive resilience governance as an ongoing process, with the information regarding incidents and operations returning to the planning and preparedness, so organizations become stable and adaptable to changing cyber and operational challenges.

**Strategic Governance Layer**

Cyber resilience governance responsibilities are included in the strategic layer that covers board and executive leadership in cyber resilience (Harizaj et al., 2025). This layer is seen to formulate strategic direction, risk appetite, resource allocation, and accountability models (Oh et al., 2025b). Among the key elements are board-level cyber risk committee having clear responsibilities and regular meeting cadence, the cyber risk appetite statements detailing the levels of disruption that can be tolerated, and recovery expectations, strategic resilience roadmap aligned with business strategy and digital transformation initiatives, executive accountability framework with clear responsibility of resilience outcomes, and periodic strategic reporting on resilience posture, results of testing, and risks(Panda & Bower, 2020; Prakesh et al., 2024). The strategic layer aligns compliance requirements

and business needs in such a way that resilience investments are tracked to organisational needs and risk tolerance. It offers the executive power and allocation of resources required to use in the face of disaster and, at the same time, the accountability offered by board control (Khaleel et al., 2025).

**Operational Governance Layer**

Strategic direction is converted into operational programmes, processes and capabilities through the operational layer. This layer involves cross-functional co-ordination, programme management and operational risk management (Halliday, 2023). This has components such as cyber resilience programme office, which coordinates all activities across functions, integrated risk management relates to links cyber risks to enterprise risk management, business continuity and crisis management integration, supply chain and third-party risk governance, and workforce capability development such as training, awareness, and specialised expertise (Cheng & Xiao, 2025). This level eliminates organisational silos based on cross-functional forms of governance in order to see cybersecurity integrated into business operations, technology decisions, and risk management as opposed to being a discrete, technical operation (Bagheri et al., 2023; Ndibe, 2025).

**Tactical Execution Layer**

The tactical layer includes day-to-day security operations, technical implementation and incident response capability. Elements are; security operations centre and continuous monitoring and threat detection; incident response team and a set of procedures and decision authority; vulnerability and patch management with risk prioritisation; identity and access management with adapting authentication; and resilience testing programme including technical testing, exercise, and validation (Verma et al., 2025; Yano et al., 2015). This layer applies the technical and operational resilience capabilities needed without compromising the regulatory requirements. It gives the operational excellence required in the prediction of threats, resistance to attacks, and recovery of events(Campbell, 2020).

**Assurance and Oversight Layer**

Independent validation, audit and continuous improvement mechanisms are offered by the assurance layer (Ebuzor, 2024). Elements are internal audit and cybersecurity expertise and resilience-oriented audit programmes; regulatory compliance oversight and reporting; independent resilience testing such as penetration testing and red team exercises; lessons learned programme involving lessons learnt through incidents and near-misses; and continuous improvement process, which involves translating lessons into capability improvements(Pham & Nguyen, 2023). The initiative under discussion will be implemented to address the challenges of preventing cybercrime and uncovering the threats. This layer guarantees that governance systems operate efficiently, that compliance requirements are fulfilled and that resiliency is achieved via an independent evaluation. It gives the feedback loops that are required to allow organisational learning and adaptation(Babeshko et al., 2024).

**Case Studies:**

This section looks at notable cybersecurity incidents that shed light on the interaction between compliance with the regulations, governance structures, and resilience ability. Both cases illustrate the extent to which organisations that passed formal compliance still had significant vulnerabilities, along with displaying some of the factors that supported or hindered successful response and recovery. Integrated governance model runs through four varied layers that are however interconnected. The top Strategic layer offers board and executive direction and oversight. Operational layer integrates cross-functional activities and the integration of enterprise risks. Day to day security operations and resilience testing are carried out at the Tactical layer. Assurance layer assures and offers continuous improvements. Top-down governance flow is represented by blue arrows, and the bottom-up learning and adaptation is facilitated by the red feedback loop. The lower panel proposes six major integration mechanisms which facilitate smooth operation of the structure.

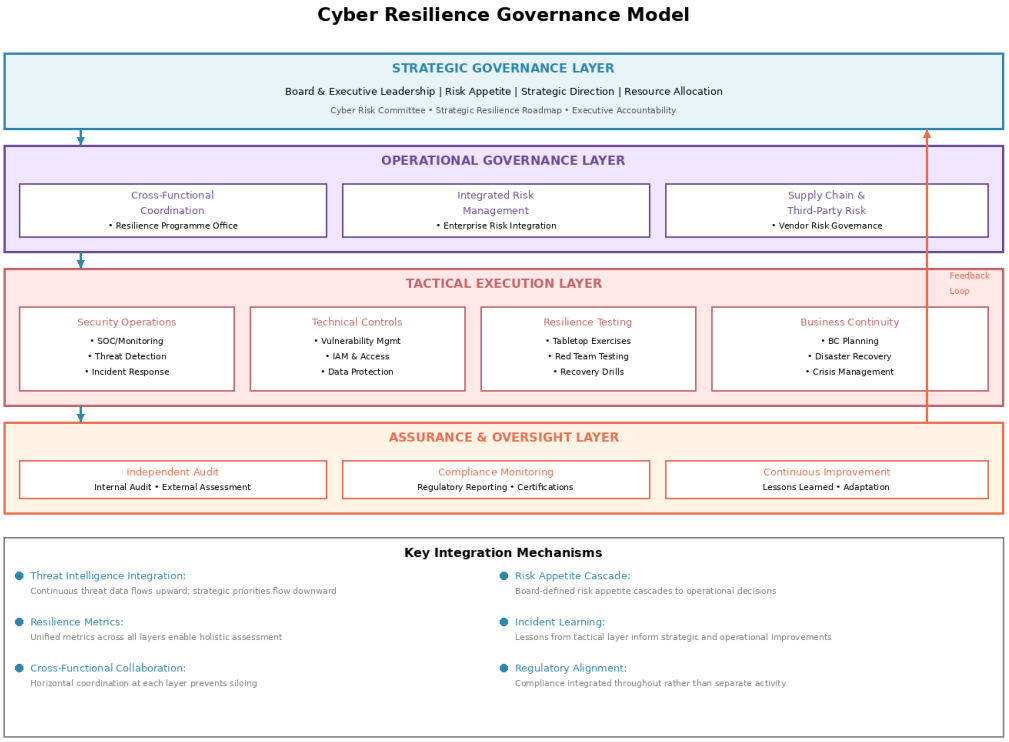


**Figure 4: Proposed Cyber Resilience Governance Model**

The figure 4, provides a Cyber Resilience Governance Model that is designed with four interrelated governance levels that transform strategic intent to operational implementation and hold accountability and a continuous improvement process. The Strategic Governance Layer is the highest layer, which provides the overall direction by board and executive leadership, establishing risk appetite, distributing resources, and establishing executive responsibility to cyber resilience. The operation of this strategy is implemented using Operational Governance Layer, which manages the cross-functional operations, integrates cyber risks into enterprise risk management, and controls supply chain and third-party risks. Under this, the Tactical Implementation Layer provides detailed security and resilience activities, including security operations, technological controls, testing resilience, and business continuity, in the case of disaster recovery and crisis management. Topping all the layers, there is the Assurance and Oversight Layer which offers independent audit, compliance monitoring, and constant improvement so that it can become effective and adaptive over the time. All levels are linked with feedback loops and integration mechanisms, threat intelligence sharing, unified resilience metrics, risk appetite cascading, incident learning, cross-functional collaboration, and regulatory alignment help all levels to ensure that cybersecurity is an integrated governance activity and not a technical activity with isolated functions to ensure that organizations continue to improve resilience to changing threats.

## Colonial Pipeline Ransomware Attack (2021)

The Colonial Pipeline ransomware is one of the most significant ransomware attacks on critical infrastructure, which impacted the fuel supply of the Eastern United States in six days(Analytica, 2021). The case is especially educative in that Colonial Pipeline had numerous regulatory frameworks such as TSA pipeline security requirements and had cybersecurity programmes that were aimed to meet these requirements. However, the network was breached by the attackers using a legacy VPN account that had no multi-factor authentication. Including the homeland security, the department of homeland security, is among the government agencies that have furthermore provided additional details on this matter (US Department of Homeland Security, 2023). Governance failures comprised the lack of IT/OT segmentation, even though it is a recognised best practice; deficiency in monitoring and detection; absence of tested incident response and recovery plans, tailored to ransomware incidents; and an operational decision to pre-emptively shut down, which represented uncertainty as to the integrity of the OT systems(Hobbs, 2021). The incident also triggered regulatory changes such as obligatory cybersecurity measures among critical pipeline operators and proved that industry-specific operational experience should be supplemented by generic requirements (Dudley & Golden, 2021; Sparkes, 2021).

**SolarWinds Supply Chain Compromise (2020)**

The SolarWinds incident is an example of a complex supply chain attack whereby hackers attacked the software build environment of a popular IT management solution and delivered malicious updates to about 18,000 clients including government agencies and Fortune 500 firms (Wolff et al., 2021). The event has significant governance repercussions, as it has shown that the conventional perimeter-based approach to security and compliance frameworks fail to provide sufficient poles on supply chain risks. The main reception was common, with it being noted that merely two out of every three businesses experience an attack annually (Huddleston et al., 2021). The general perception was typical, as two out of three companies have been reported to be subjected to an attack each year (Ghanbari et al., 2024). Among the lessons presented by governance, are the limitations of traditional vendor risk assessments due to their emphasis on contractual compliance over security practices; the risk posed by software monocultures, aggregation by vendors; the difficulty of identifying advanced patient adversaries who are insiders in trusted systems; and the systemic characteristics of supply chain risk that cannot be managed by individual organisational policies (Martínez & Durán, 2021).

**Healthcare Sector Ransomware Epidemic**

Despite the widespread HIPAA compliance, the healthcare sector has witnessed ongoing, grave ransomware assaults on hospitals, health care systems, and medical equipment producers. All of these occurrences overall indicate that compliance with HIPAA, despite its creation of minimum security standards, is ineffective against the modern-day threat environment(Minnaar & Herbig, 2021). Specific governance gaps in healthcare are distinct operational limitations that make security implementation more difficult; resource limitations especially small community hospitals; fragmented IT infrastructure across multiple vendors and systems; and incident response issues when operational failure poses a direct threat to patient safety (Neprash et al., 2022). The lessons on resilience highlight the paramount role of business continuity planning that ensures patient care capabilities in the time of IT outages, paper-based backup processes, and quick recovery capabilities (Stachtiaris, 2022).

**Table 3: Comparative Case Study Analysis**

| Incident | Regulatory Context | Governance Failure | Resilience Gap | Key Lesson |
|---|---|---|---|---|
| **Colonial Pipeline** | TSA Pipeline Security | IT/OT segmentation; legacy systems | Untested incident response | Resilience testing must include ransomware scenarios |
| **SolarWinds** | Multiple frameworks; SOC 2 | Build environment security; software integrity | Detection against sophisticated adversaries | Supply chain risks require systemic governance |
| **Healthcare Ransomware** | HIPAA Security Rule | Resource constraints; legacy systems | Business continuity for life-critical operations | Sector-specific constraints require tailored resilience |

The table 3, presents three significant cybersecurity incidents on the basis of how regulatory compliance is not sufficient to achieve operational resilience with the focus made on the governance and resilience gaps that are evident in each instance. At the Colonial Pipeline incident, adherence to the TSA pipeline security requirements was insufficient to prevent operational disruption, and governance weaknesses (poor IT/OT segmentation and use of legacy systems) compounded the problem, whereas the lack of incident response plans test failed to indicate resilience failures, reflecting the fact that resilience exercises need to be spelt out to include ransomware scenarios. The SolarWinds breach of supply chain happened in organizations that are already compliant with various frameworks such as SOC 2 but governance lapses in securing software development environments and protecting software integrity enabled attackers to compromise trusted systems, suggesting a resilience void in identifying the existence of highly advanced adversaries and the necessity of systemically managing supply chain risks. Likewise, the continued ransomware attacks in the healthcare sector in spite of HIPAA compliance demonstrate that the resource constraints and outdated infrastructure pose challenges to proper governance, and that lack of business continuity planning endangers the life-critical healthcare activities, showing that operational specificities of the sector need specific resilience

plans and not universal compliance. Comprehensively, the comparison illustrates that the maturity and resilience capabilities in governance are to be transformed to go beyond compliance in the regulations to respond to the real-life operational risks.

**Discussion: Policy and Practice Implications**

The regulation framework and gap analysis as well as case studies analysis discloses some important insights that can have an impact on policymakers, organisational leaders, and cybersecurity researchers. This part summarises research and examines its theoretical and practical implications.

**Regulatory Design Implications**

The study reveals that good cybersecurity regulation is one that goes beyond conventional compliance paradigms to models that expressly develop resilience capacity(Idengren, 2024). This involves a number of regulatory reorientations. First, regulations must embrace outcome-based requirements, which define resilience goals, including maximum tolerable disruption periods, or recovery time goals, as opposed to defining technical controls. Second, the legislation ought to require validation of resilience capabilities by testing requirements(Adabara et al., 2025). The regulations ought to include specific learning requirements, which would involve systematic post-incident analysis and an indication of improvements.

The study shows that efficient cybersecurity regulation should not be limited to conventional approaches of compliance but should be implemented in frameworks that clearly develop resilience capacities. This entails a number of changes in regulation strategy. One, the regulations must embrace the use of outcome-based requirements that lay down the resilience goals. Second, the regulations are to be required to be validated by testing. Third, they are to include clear learning requirements.

**Organisational Governance Implications**

The study notes that regulatory compliance, though required, is not enough to ensure cyber resilience in organisational leaders. The boards and corporate leaders need to rebrand cybersecurity as a technical compliance requirement to a strategic capability that needs active management. The governance at the board level should move further than the compliance monitoring to the strategic resilience management (Hassan et al., 2022). This demands that boards build cyber literacy, reporting on resilience capabilities, engage in planning skills and resources must be sufficient. Executive management tends to consider cybersecurity as a technical issue to be assigned to and not a strategic risk to be addressed proactively (Zaki, 2025). The study has shown that the executive should be involved in resilience governance, especially when it comes to resource distribution, cross-functional integration, and crisis decision-making. Good resilience entails top management that is aware of cyber risks and capable of expressing risk appetite as well as being an advocate of organisational culture that builds resilience rather than compliance.

**Policy and Managerial Recommendations**

Based on the research findings, this section provides specific, actionable recommendations for different stakeholder groups involved in cybersecurity governance.

**Recommendations for Governments and Regulators**

Evolve regulatory frameworks toward outcome-based requirements that specify resilience objectives rather than prescriptive technical controls.

Mandate resilience validation through regular testing including scenario-based exercises and threat-led penetration testing (National Cyber Security Centre, 2022).

Establish sector-level resilience coordination mechanisms addressing systemic risks from interconnections.

Harmonise overlapping regulatory requirements across jurisdictions to reduce compliance complexity.

Incentivise proactive resilience investment through regulatory recognition programmes.

**Recommendations for Boards and Executive Leadership**

Establish board-level cyber risk committees with defined responsibilities for resilience oversight.

Define explicit cyber risk appetite statements specifying tolerable disruption levels and recovery expectations.

Participate actively in resilience testing exercises including crisis simulation tabletops.

Ensure reporting frameworks provide visibility into resilience capabilities rather than merely compliance status.

Allocate resources explicitly for resilience capabilities beyond baseline compliance requirements.

**Recommendations for CISOs and Security Leaders**

Reframe security programmes around resilience capabilities rather than compliance requirements.

Implement continuous resilience validation through regular technical testing and exercises.

Establish systematic incident learning processes with root cause analysis and improvement tracking.

Develop resilience metrics complementing compliance indicators.

Foster cross-functional collaboration integrating cybersecurity with business continuity and risk management.

## Conclusion

The study has explored the root cause of the lack of alignment between regulatory compliance and cyber resilience, that there exist regulatory governance gaps that expose organisations despite seeming to comply with regulations and postulate an integrated governance system that links the compliance requirements with resilience principles. By conducting a comparative analysis of the key regulatory frameworks, a systematic analysis of the existing regulatory gaps, and investigations of the most notable cases, we have shown that the existing compliance-oriented strategies is a necessary but ineffective tool to achieve real cyber resilience. The study discloses a number of vital findings. First, even though regulatory frameworks have changed dramatically, there still exist inherent gaps in terms of adapting governance, incident learning, supply chain risks, and demonstrating resilience capacity. Second, these gaps show more underlying tensions on compliance paradigms that focus on documentation versus resilience paradigms that need adaptive capacity. Third, the solution to these gaps lies in radical changes in the way organisations conceptualise, govern and operationalise cybersecurity.

The given Cyber Resilience Governance Framework provides an organized way to achieve this change by harmonising the compliance requirements and resilience capacity by using four connected layers of governance. The framework fills the gaps found by integrating adaptive risk management, organisational learning, supply chain resilience, human factors integration, and testing validation. The applications in practice can be found in a variety of stakeholder groups. To the policymakers and regulators, the study reveals the necessity of regulatory transformation to outcome-based requirements and resilience validation requirements. To organisational leaders and boards, it emphasises the urgent need to have active cyber risk governance that goes beyond compliance monitoring. It also offers systematic advice to security practitioners on how to shift towards resiliency oriented capabilities. These challenges remain in high demand. Cyber threats become more innovative and impactful. The digital transformation increases faster, which provides more attack surfaces. Systemic risks are created by critical infrastructure vulnerabilities. In these terms, the fact that compliance is being replaced by resilience is not just a governance enhancement but a strategic necessity to the survival of organisations, economic sustainability and even national security.

## References

[1] Adabara, I., Sadiq, B. O., Shuaibu, A. N., Danjuma, Y. I., & Venkateswarlu, M. (2025). A Review of Agentic AI in Cybersecurity: Cognitive Autonomy, Ethical Governance, and Quantum-Resilient Defense. F1000Research, 14, 843.

[2] Agarwal, K., & Shah, M. (2024). The Role of Corporate Governance in Managing Cybersecurity Risks: A Comprehensive Analysis. LawFoyer Int'l J. Doctrinal Legal Rsch., 2, 352.

[3] Aghazadeh Ardebili, A., Lezzi, M., & Pourmadadkar, M. (2024). Risk Assessment for Cyber Resilience of Critical Infrastructures: Methods, Governance, and Standards. Applied Sciences, 14(24), 11807.

[4] Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2020). How integration of cyber security management and incident response enables organizational learning. Journal of the Association for Information Science and Technology, 71(8), 939–953. https://doi.org/10.1002/asi.24311

[5] Akinsola, K. (2025). The Role of Corporate Governance in Strengthening Compliance Frameworks. Available at SSRN 5126938. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5126938

[6] Alrehili, A. A., & Alhazmi, O. H. (2024). ISO/IEC 27001 Standard: Analytical and Comparative Overview. In S. Das, S. Saha, C. A. Coello Coello, & J. C. Bansal (Eds.), Advances in Data-Driven Computing and Intelligent Systems (Vol. 891, pp. 143–156). Springer Nature Singapore. https://doi.org/10.1007/978-981-99-9524-0_12

[7] Alshar'e, M. (2023). Cyber security framework selection: Comparision of NIST and ISO27001. Applied Computing Journal, 245–255.

[8] Analytica, O. (2021). Us pipeline hack to make ransomware risks a priority. Emerald Expert Briefings, (oxan-ga).

[9] Anil, V. K. S., & Babatope, A. B. (2024a). The role of data governance in enhancing cybersecurity resilience for global enterprises. World J. Adv. Res. Rev, 24(1). https://www.researchgate.net/profile/Adeoluwa-Babatope/publication/385173901_The_Role_of_Data_Governance_in_Enhancing_Cybersecurity_Resilience_for_Global_Enterprises/links/671befc255a5271cdeda1e79/The-Role-of-Data-Governance-in-Enhancing-Cybersecurity-Resilience-for-Global-Enterprises.pdf

[10] Anil, V. K. S., & Babatope, A. B. (2024b). The role of data governance in enhancing cybersecurity resilience for global enterprises. World J. Adv. Res. Rev, 24(1).

[11] Azmi, R., Tibben, W., & Win, K. T. (2018). Review of cybersecurity frameworks: Context and shared concepts. Journal of Cyber Policy, 3(2), 258–283.

[12] Babeshko, E., Illiashenko, O., Kharchenko, V., Morozova, O., Paturej, A., Paturej, K., Peña, E., Potii, O., & Rapacki, Z. (2024). Manual on cybersecurity, reliability and resilience assurance in the critical industries. International Centre for Chemical Safety and Security.

[13] Bagheri, S., Ridley, G., & Williams, B. (2023). Organisational cyber resilience: Management perspectives. Australasian Journal of Information Systems, 27.

[14] Bahmanova, A., & Lace, N. (2026). Modelling Cyber Resilience in SMEs as a Socio-Technical System: A Systemic Approach to Adaptive Digital Risk Management. Systems, 14(2), 151.

[15] Bima, S., & Intan, W. (2024). INTEGRATING CYBER INCIDENT RESPONSE WITH DISASTER RECOVERY FOR ENHANCED ORGANIZATIONAL RESILIENCE. Manuscripts on the Artificial Intelligence and Digital Research, 1(2), 68–77.

[16] Boddy, S. E. (2024). Case study: The decision-support framework and NIS2, CER, and DORA incident reporting obligations. https://jyx.jyu.fi/jyx/Record/jyx_123456789_95795

[17] Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., & Filar, B. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. arXiv Preprint arXiv:1802.07228.

[18] Buttigieg, C. P., & Zimmermann, B. B. (2024). The digital operational resilience act: Challenges and some reflections on the adequacy of Europe's architecture for financial supervision. ERA Forum, 25(1), 11–28. https://doi.org/10.1007/s12027-024-00793-w

[19] Calder, A. (2018). NIST Cybersecurity Framework: A pocket guide. IT Governance Publishing Ltd. https://books.google.com/books?hl=en&lr=&id=rWxvDwAAQBAJ&oi=fnd&pg=PT8&dq=nist+cybersecurity+framework+csf&ots=q_nZaQyuun&sig=dYDM6Haa72l4qE_ZFgA6QIthxok

[20] Calder, A. (2020). Information Security based on ISO 27001/ISO 27002. Van Haren. https://books.google.com/books?hl=en&lr=&id=yhJADwAAQBAJ&oi=fnd&pg=PA1&dq=ISO/IEC+27001+and+27002&ots=sJFT0ZZsaX&sig=n2bJHoYg6IzOA2Ac2-qqhe6YBwU

[21] Campbell, R. (2020). The need for cyber resilient enterprise distributed ledger risk management framework. The Journal of The British Blockchain Association.

[22] Carías, J. F., Arrizabalaga, S., Labaka, L., & Hernantes, J. (2020). Cyber resilience progression model. Applied Sciences, 10(21), 7393.

[23] Cheng, L., & Xiao, Y. (2025). From space to law: A five-layer construction of cyber governance. International Journal of Legal Discourse, 10(2), 251–282.

[24] Choi, S.-H., Youn, J., Kim, K., Lee, S., Kwon, O.-J., & Shin, D. (2023). Cyber-resilience evaluation methods focusing on response time to cyber infringement. Sustainability, 15(18), 13404.

[25] Christine, D. I., & Thinyane, M. (2022). Socio-technical cyber resilience: A systematic review of cyber resilience management frameworks. Digital Transformation for Sustainability: ICT-Supported Environmental Socio-Economic Development, 573–597.

[26] Clausmeier, D. (2023). Regulation of the European Parliament and the Council on digital operational resilience for the financial sector (DORA). International Cybersecurity Law Review, 4(1), 79–90. https://doi.org/10.1365/s43439-022-00076-5

[27] Conklin, W. A., & Shoemaker, D. (2017). Cyber-resilience: Seven steps for institutional survival. EDPACS, 55(2), 14–22.

[28] Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. Journal of Information Security, 4(2). https://serwiss.bib.hs-hannover.de/files/938/ISOIEC_27000_27001_and_27002_for_Information_Security_Management.pdf

[29] Dudley, R., & Golden, D. (2021). The colonial pipeline ransomware hackers had a secret weapon: Self-promoting cybersecurity firms. ProPublica (24 May 2021).
[30] Dupont, B. (2012). The cyber security environment to 2022: Trends, drivers and implications. Drivers and Implications. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2208548
[31] Ebuzor, J. (2024). Good Governance and Cybersecurity: Enhancing Digital Resilience. In Corporate Cybersecurity in the Aviation, Tourism, and Hospitality Sector (pp. 112–136). IGI Global.
[32] Espinoza, F., Maryska, M., Doucek, P., & Kovářova, M. (2023). DORA and NIS2 and their Impact on Database Security. IDIMT-2023: New Challenges for ICT and Management. https://epub.jku.at/urn/urn:nbn:at:at-ubl:3-20510
[33] Fan, X. (2024). Between fragmentation and integration: The United Nations and global cybersecurity regulation.
[34] Faruq, M. O., & Mollah, M. H.-O.-R. (2021). POST-GDPR DIGITAL COMPLIANCE IN MULTINATIONAL ORGANIZATIONS: BRIDGING LEGAL OBLIGATIONS WITH CYBERSECURITY GOVERNANCE. American Journal of Scholarly Research and Innovation, 1(01), 27–60.
[35] Folorunso, A., Wada, I., Samuel, B., & Mohammed, V. (2024). Security compliance and its implication for cybersecurity. World Journal of Advanced Research and Reviews, 24(01), 2105–2121.
[36] Ghanbari, H., Koskinen, K., & Wei, Y. (2024). From SolarWinds to Kaseya: The rise of supply chain attacks in a digital world. Journal of Information Technology Teaching Cases, 20438869241299823.
[37] Gómez, L., Vander Peterson, C., Rojas, M., & Pereira, A. (2025). A Risk-Based Approach to Cybersecurity Governance and Management: Strengthening Information Assurance Through Policy Development, Compliance Measures, and Technical Controls. Annual Review of Foundational and Emerging Scientific Methodologies, 15(6), 1–14.
[38] Halliday, N. (2023). A conceptual framework for financial network resilience integrating cybersecurity, risk management and digital infrastructure stability. International Journal of Advanced Multidisciplinary Research and Studies, 3, 1253–1263.
[39] Harizaj, M., Qafa, R., & Idrizi, O. (2025). Strategic Vulnerability Analysis of Cybersecurity Frameworks: Toward a Hybrid Model for Governance and Resilience. International Conference on Intelligence-Based Transformations of Technology and Business Trends, 84–96.
[40] Hassan, M. K., Abdulkarim, M. E., & Ismael, H. R. (2022). Risk governance: Exploring the role of organisational culture. Journal of Accounting & Organizational Change, 18(1), 77–99.
[41] Heim, T. N. (2023). Global governance and regulation of cybersecurity: Towards coherence or fragmentation? https://research.utwente.nl/en/publications/global-governance-and-regulation-of-cybersecurity-towards-coheren
[42] Hobbs, A. (2021). The colonial pipeline hack: Exposing vulnerabilities in us cybersecurity. SAGE Publications: SAGE Business Cases Originals.
[43] Hossain, M. S., Hasan, H. M., & Akter, F. (2022). ENHANCING CYBER RESILIENCE IN GOVERNMENT INSTITUTIONS, A COMPARATIVE ANALYSIS OF POLICY FRAMEWORKS ACROSS DEVELOPING AND DEVELOPED NATIONS. International Journal Of Engineering Technology Research & Management (IJETRM), 6(10), 117–125.
[44] Huber, S., van Wijgerden, I., de Witt, A., & Dekker, S. W. (2009). Learning from organizational incidents: Resilience engineering for high-risk process environments. Process Safety Progress, 28(1), 90–95.
[45] Huddleston, J., Ji, P., Bhunia, S., & Cogan, J. (2021). How vmware exploits contributed to solarwinds supply-chain attack. 2021 International Conference on Computational Science and Computational Intelligence (CSCI), 760–765.
[46] Idengren, P. (2024). Cybersecurity and the resilience measures in critical infrastructure in sweden: A comparative desk study between sweden and the united states.
[47] ISO 27000. (2009). Information Technology, Security Techniques, Information Security Management Systems, Overview and Vocabulary," International Organization for Standardization ISO, Geneve, 2009.
[48] Itani, D., Itani, R., Eltweri, A. A., Faccia, A., & Wanganoo, L. (2024). Enhancing cybersecurity through compliance and auditing: A strategic approach to resilience. 2024 2nd International Conference on Cyber Resilience (ICCR), 1–10.
[49] Ivaščevs, A., Parfjonovs, A., Augustāne, L., Eglītis, R., & Bikovska, J. (2025). Challenges and First Lessons Learned for NIS2: Directive Implementation in Banking Sector. 2025 66th International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS), 1–7. https://ieeexplore.ieee.org/abstract/document/11236569/
[50] Kala, E. M. (2024). Public-Private Synergy in Cybersecurity Advanced Strategies for Bridging Regulatory Gaps and Enhancing Digital Resilience. International Journal of Research, 10(2), 31–40.
[51] Khaleel, M., Yusupov, Z., El-Khozondar, H. J., & Alsharif, A. (2025). Cyber-Resilience Strategies for Smart Microgrids: Classification, Construction, Recent Trends, and Policy Framework. Int. J. Electr. Eng. and Sustain., 31–47.
[52] Kharlamov, A., & Pogrebna, G. (2021). Using human values-based approach to understand cross-cultural commitment toward regulation and governance of cybersecurity. Regulation & Governance, 15(3), 709–724.
[53] Lichte, D., Torres, F. S., & Engler, E. (2022). Framework for operational resilience management of critical infrastructures and organizations. Infrastructures, 7(5), 70.

[54] Lone, A. N., Mustajab, S., & Alam, M. (2023). A comprehensive study on cybersecurity challenges and opportunities in the IOT world. SECURITY AND PRIVACY, 6(6), e318. https://doi.org/10.1002/spy2.318

[55] Loumachi, F. Y., Lacerda, M., Ouazzane, K., Adnane, A., & Adamyk, O. (2025). AI in Control: Rethinking Cybersecurity Compliance and Auditing. Available at SSRN 5731707. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5731707

[56] Martínez, J., & Durán, J. M. (2021). Software supply chain attacks, a threat to global cybersecurity: SolarWinds' case study. International Journal of Safety and Security Engineering, 11(5), 537–545.

[57] Mehmood, K. T., Ashraf, Z., Iqbal, R., Rafique, A. A., Gul, H., & Ali, M. (2025). Cyber security Governance as a Pillar of Enterprise Risk Management: Designing a Compliance-Driven Framework for Operational Resilience, Policy Enforcement, and Regulatory Alignment. Annual Methodological Archive Research Review, 3(5), 59–77.

[58] Melaku, H. M. (2023a). A dynamic and adaptive cybersecurity governance framework. Journal of Cybersecurity and Privacy, 3(3), 327–350.

[59] Melaku, H. M. (2023b). A dynamic and adaptive cybersecurity governance framework. Journal of Cybersecurity and Privacy, 3(3), 327–350.

[60] Melaku, H. M. (2023c). A dynamic and adaptive cybersecurity governance framework. Journal of Cybersecurity and Privacy, 3(3), 327–350.

[61] Minnaar, A., & Herbig, F. J. (2021). Cyberattacks and the cybercrime threat of ransomware to hospitals and healthcare services during the COVID-19 pandemic. Acta Criminologica: African Journal of Criminology & Victimology, 34(3), 155–185.

[62] Möller, D. P. F. (2023). NIST Cybersecurity Framework and MITRE Cybersecurity Criteria. In D. P. F. Möller, Guide to Cybersecurity in Digital Transformation (Vol. 103, pp. 231–271). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-26845-8_5

[63] National Cyber Security Centre. (2022). Cyber Security Toolkit for Boards. London: NCSC.

[64] Ndibe, O. S. (2025). CYBER-ALIGNTM Maturity Index: A Multi-Dimensional Evaluation Framework for Measurable Cyber Resilience Across Governance, Human Behavior, and Operational Controls. Human Behavior, and Operational Controls (October 29, 2025).

[65] Neprash, H. T., McGlave, C. C., Cross, D. A., Virnig, B. A., Puskarich, M. A., Huling, J. D., Rozenshtein, A. Z., & Nikpay, S. S. (2022). Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016-2021. JAMA Health Forum, 3(12), e224873–e224873.

[66] Novokreshchenova, D. K. (2025). Operationalizing Cybersecurity Resilience in Small and Medium Enterprises: An Integrated Analysis of Adaptive Maturity Models, Managed Threat Response, and Regulatory Compliance. European Index Library of European International Journal of Multidisciplinary Research and Management Studies, 5(10), 41–46.

[67] Obioha-Val, O. A. (2025). Bridging gaps in cybersecurity governance: Leveraging collaborative digital solutions. Asian Journal of Research in Computer Science, 18(2), 82–100.

[68] Oh, K. B., Hoang, G., Sturdy, J., & Guo, S. S. (2025a). Cybersecurity and Governance. In K. B. Oh, G. Hoang, J. Sturdy, & S. S. Guo, Cybersecurity Governance (pp. 19–63). Springer Nature Singapore. https://doi.org/10.1007/978-981-95-3865-2_2

[69] Oh, K. B., Hoang, G., Sturdy, J., & Guo, S. S. (2025b). Strategic Cybersecurity Governance. In Cybersecurity Governance: An Enterprise Risk Management Strategy for Cyber Risk Control (pp. 215–260). Springer.

[70] Omolere, O. (2025). Cybersecurity Risk Assessment And Audit Frameworks: A Study Of Compliance And Governance. Available at SSRN 6059757. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=6059757

[71] Ositashvili, M. (2024). The key role of the most recent EU regulation–the "Digital Operational Resilence Act" in the legal system, contemporary challenges, and Georgian perspectives. ESI Preprints (European Scientific Journal, ESJ), 20(26), 1–1.

[72] Panda, A., & Bower, A. (2020). Cyber security and the disaster resilience framework. International Journal of Disaster Resilience in the Built Environment, 11(4), 507–518.

[73] Pemmasani, P. K. (2023). National cybersecurity frameworks for critical infrastructure: Lessons from governmental cyber resilience initiatives. International Journal of Acta Informatica, 2(1), 209–218.

[74] Pham, M. T., & Nguyen, L. H. (2023). A Comparative Review of Cybersecurity Standards and Frameworks: Supporting Information Assurance in Government and Industry Systems. Transactions on Machine Learning, Artificial Intelligence, and Advanced Intelligent Systems, 13(8), 1–15.

[75] Popoola, A. D., & Ibrahim, A. K. (2024). Conceptual Framework for Strengthening Governance and Compliance in Enterprise Financial Systems. International Journal of Advanced Multidisciplinary Research and Studies, 4. https://www.multiresearchjournal.com/admin/uploads/archives/archive-1766046814.pdf

[76] Prakesh, V., Khare, S., Talwandi, N. S., Surender, Lalar, S., & Thakur, P. (2024). Strategic Framework Form Cybersecurity Risk Management: Enhancing Resilience in an Evolving Threat Landscape. International Conference on Recent Developments in Cyber Security, 173–183.

[77] Qudus, L. (2025). Cybersecurity governance: Strengthening policy frameworks to address global cybercrime and data privacy challenges. International Journal of Science and Research Archive, 14(1), 1146–1163.

[78] Rajola, F., Gatelli, P., & Iacopino, V. (2025). Governance Processes and Technologies for Cyber Resilience in the Financial Sector: The Italian Scenario. Information Systems Journal.
[79] Rezazade Mehrizi, M. H., Nicolini, D., & Modol, J. R. (2022). How do organizations learn from information system incidents? A synthesis of the past, present, and future. MIS Quarterly, 46(1), 531–590.
[80] Sabidi, M. L., & Zolkipli, M. F. (2024). The Role of Risk Management in Cybersecurity Protocols. Borneo International Journal eISSN 2636-9826, 7(2), 77–81.
[81] Sharma, D., Reddy, S., & Shahid, H. (2023). Cybersecurity Obligations for Critical Infrastructure: Emerging Legal Norms, Enforcement Gaps, and Governance Challenges. Legal Studies in Digital Age, 2(3), 49–63.
[82] Shrestha, A. (2025). A Strategic Framework for Strengthening Cyber Risk Governance and Resilience in US Critical Infrastructure Sectors. Applied Sciences, Computing, and Energy, 3(3), 512–527.
[83] Singh, H. (2025a). The Importance of Cybersecurity Frameworks and Constant Audits for Identifying Gaps, Meeting Regulatory and Compliance Standards. Meeting Regulatory and Compliance Standards (May 23, 2025). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5267862
[84] Singh, H. (2025b). The Importance of Cybersecurity Frameworks and Constant Audits for Identifying Gaps, Meeting Regulatory and Compliance Standards. Meeting Regulatory and Compliance Standards (May 23, 2025). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5267862
[85] Sparkes, M. (2021). How do we solve the problem of ransomware? Elsevier.
[86] Stachtiaris, E. (2022). Hacking healthcare: Ransomware as a rising contagion. Hofstra L. Rev., 51, 1117.
[87] Sulich, A., Rutkowska, M., Krawczyk-Jezierska, A., Jezierski, J., & Zema, T. (2021). Cybersecurity and sustainable development. Procedia Computer Science, 192, 20–28.
[88] Svantesson, D. J. B. (2021). Private international law and the internet.
[89] Taylor, R. H., Weyman, A., Carhart, N. J., Voke, R. C., & May, J. H. (2021). Achieving greater resilience to major events: Organisational learning for safety risk management in complex environments.
[90] Thakur, K., & Pathan, A.-S. K. (2020). Cybersecurity fundamentals: A real-world perspective. CRC Press. https://www.taylorfrancis.com/books/mono/10.1201/9781003035626/cybersecurity-fundamentals-kutub-thakur-al-sakib-khan-pathan
[91] Uddoh, J., Ajiga, D., Okare, B. P., & Aduloju, T. D. (2021). Digital resilience benchmarking models for assessing operational stability in high-risk, compliance-driven organizations. Int J Multidiscip Res Growth Eval, 2(3), 598–606.
[92] US Department of Homeland Security. (2023). Cross-Sector Cybersecurity Performance Goals. Washington, DC: CISA.
[93] U.S. Department of Homeland Security. (2023). Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act). Washington, DC: DHS.
[94] Vandezande, N. (2024). Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor. Computer Law & Security Review, 52, 105890.
[95] Verma, P., Newe, T., O'Mahony, G. D., Brennan, D., & O'Shea, D. (2025). Towards a Unified Understanding of Cyber Resilience: A Comprehensive Review of Concepts, Strategies, and Future Directions. IEEE Access.
[96] Viscardi, V. (2020). The Influence of National Cultures on Cybersecurity Strategies: A Comparative Case Studies analysis of the UK and Italy's Cybersecurity Postures.
[97] White, G. B., & Sjelin, N. (2022). The NIST cybersecurity framework. In Research anthology on business aspects of cybersecurity (pp. 39–55). IGI Global. https://www.igi-global.com/chapter/the-nist-cybersecurity-framework/288672
[98] Wolff, E. D., GroWlEy, K. M., Lerner, M. O., Welling, M. B., Gruden, M. G., & Canter, J. (2021). Navigating the solarwinds supply chain attack. Procurement Law., 56, 3.
[99] Yano, E. T., De Abreu, W., Gustavsson, P. M., & Åhlfeldt, R.-M. (2015). A framework to support the development of cyber resiliency with situational awareness capability. 20th International Command and Control Research and Technology Symposium, June, 16–19.
[100] Young, R. G. (2025a). Cyber Resilience in Banking: A Practical Guide to Governance, Risk, and Compliance. CRC Press. https://books.google.com/books?hl=en&lr=&id=_I2NEQAAQBAJ&oi=fnd&pg=PA1956&dq=From+Compliance+to+Cyber+Resilience:+Bridging+Governance+Gaps+in+Regulatory+Cybersecurity+Frameworks&ots=D2Hr-suhSo&sig=zhydKoDDuHD3yG2aWSmLcXNTJ08
[101] Young, R. G. (2025b). Cyber Resilience in Banking: A Practical Guide to Governance, Risk, and Compliance. CRC Press.
[102] Zaki, B. L. (2025). Conceptualising organisational policy learning: Triggers, processes, outcomes, and implications for policy and governance change. Australian Journal of Public Administration, 1467-8500.70031. https://doi.org/10.1111/1467-8500.70031
[103] Zamil, M. H., & Faruq, M. O. (2022). Cybersecurity And Data Integrity in Financial Systems: A Review Of Risk Mitigation And Compliance Models. International Journal of Scientific Interdisciplinary Research, 1(01), 27–61.
[104] Zarrabi Jorshari, F. (2016). A semantic based framework for software regulatory compliance [PhD Thesis, University of East London]. https://uel-repository.worktribe.com/file/482783/1/Fatemeh%20Zarrabi%20Jorshari%20E.pdf

[105] Zighan, S. (2024). Navigating the cyber landscape: A framework for transitioning from business continuity to digital resilience. 2024 2nd International Conference on Cyber Resilience (ICCR), 01–06.