SJIF Impact Factor (2026): 8.863| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 11 | Issue: 3 | March 2026 - Peer Reviewed Journal

COMPARATIVE ANALYSIS OF CYBERSECURITY GOVERNANCE MODELS ACROSS INDUSTRIES

Karyn Ekpo[1]
[1]*University of West Georgia – Richards College of Business, Georgia, USA*

Article DOI: https://doi.org/10.36713/epra26769
DOI No: 10.36713/epra26769

ABSTRACT
Cybersecurity is an essential governance issue in industries in the United States, yet governance models lack homogeneity and maturity. This paper provides an integrative comparative analysis of cybersecurity governance in five domains, namely financial services, healthcare, energy and operational technology (OT), local government, and higher education. Based on global frameworks (ISO/IEC 27001, NIST Cybersecurity Framework, COBIT 2019), sectoral maturity models, and empirical reviews in recent literature, the research analyzes how boards, executives, and risk functions organize their responsibilities, coordinate their frameworks, and react to regulatory pressure. The convergence around a limited number of multi-framework stacks and governance-risk-compliance logics is demonstrated by the analysis, but the analysis also identifies divergences based on regulatory intensity, resource constraints, organizational culture, and variations in risk profiles (data-centric and safety-critical environments). The public and education sectors, especially, which are under-resourced, find it hard to bring the formal responsibilities to actual practice. The article suggests a three-tier integrative reference model of cybersecurity governance that is aligned to the framework and sensitive sector and points out new requirements to govern AI-enabled security capabilities in addition to traditional controls.
KEYWORDS: *Cybersecurity Governance, NIST Cybersecurity Framework, ISO/IEC 27001, Critical Infrastructure.*

1. INTRODUCTION

Cybersecurity risk has ceased to be a domain of technical specialists and has now become a structural governance imperative (Ekpo, K., 2026). The growing threat activity, accelerated digitalization, going to the cloud, and globally distributed supply chains have transformed cyber risk into an organization-wide and persistent challenge that even highly mature businesses cannot escape (Essien et al., 2022). On the board level, cyber risk has become one of the most important enterprise risks, and the most influential governance organizations suggest that it should be addressed at the same level as financial and strategic risks instead of being assigned to IT (World Economic Forum, 2021).

Cybersecurity is defined by technical standards and its critical role in societal stability. NIST and ISO focus on the security of information and the digital infrastructure, and define cybersecurity as the protection of society, individuals, organizations, and countries against cyber risk (Hossain et al., 2024). The wider prism suggests that cybersecurity governance should be linked in terms of operational controls, regulatory compliance, enterprise risk management, and trust of digital services by the citizens. In this context, governance relates to the fact that cyber risk is no longer an issue that is handled as a technical activity but rather as an enterprise-wide strategic issue (Essien et al., 2022).

In the United States and other countries, organizations have turned to a network of voluntary structures as a way to frame this challenge. The ISO/IEC 27001, the NIST Cybersecurity Framework (CSF), COBIT 2019, COSO, CIS Controls and ITIL all dominate the mapping of the systematic reviews (Reuben-Owoh and Haig, 2025). These models vary in their breadth, cost, certification possibilities and orientation towards governance, but are often used in combination and not in isolation. According to alignment work, ISO/IEC 27001 recommends prescriptive, certifiable controls; NIST CSF is a flexible, risk-based operational model; and COBIT provides strategic governance and performance control in the field of enterprise IT and risk management (Essien et al., 2022). This multi-framework stack is especially relevant to U.S. organizations, as the NIST CSF was originally created to help oversee U.S. critical infrastructure, and since then, it has been extensively used across industries and has been combined with ISO, COBIT as well as COSO style enterprise governance.

Reviews based on sectors demonstrate, though, that generic frameworks are not adequate. The cybersecurity frameworks in this case should be both broad and flexible to open and decentralized academic settings in higher education, where awareness and training, policy compliance measures, and constant improvement are the key elements (Barruga, 2025). Though local governments are rapidly digitizing and implementing smart-city strategies, they are not adequately resourced, are susceptible to cyberattacks, and do not have specific

SJIF Impact Factor (2026): 8.863| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 11 | Issue: 3 | March 2026 - Peer Reviewed Journal

advice on how to integrate cybersecurity into their governance systems (Hossain et al., 2024, 2025). These results indicate the existence of a sustained disconnect between frameworks that are popularly disseminated and the ability of public and quasi-public organizations to adopt it.

New studies also indicate that the models of cybersecurity governance will have to be updated to fit AI-enabled functionality. Large language models (LLMs) have the potential to support various threat-modelling approaches, which enhance accessibility and repeatability of risk analysis, but also pose novel challenges of quality of data, regulatory congruity and sustainable digital infrastructure (Jersic et al., 2025). Recent achievements in integrated blockchain-AI-legal models also place advanced technologies as the means of implementing such policies, helping to demonstrate compliance and determining what risk level is acceptable (Toapanta et al., 2025). As the U.S. industries are simultaneously under pressure due to AI implementation, dynamic cyber regulation, and risk profiles specific to the sector, the developments increase the necessity of cross-sector understanding of governance structures.

The combination of existing literature demonstrates three patterns. The first is that cross-industry models like ISO/IEC 27001, NIST CSF, COBIT 2019, COSO and ITIL have an extensive toolbox of governance and control practices, and the alignment across models is becoming increasingly vital compared to adherence to any one standard (Essien et al., 2022; Reuben-Owoh and Haig, 2025). Second, higher education and local government reviews make it clear that governance models must be contextualized to organizational structures, cultures and regulatory environment, which in many cases are less developed in the public and quasi-public sectors (Hossain et al., 2024, 2025; Barruga, 2025). Third, AI- and LLM-based solutions are starting to supplement the conventional structures, yet their role in formal governance, particularly in the perspectives of boards and regulators, has not been resolved yet (Jersic et al., 2025; Toapanta et al., 2025). Although recent trends in the sectoral and framework-centric scholarship have begun to emerge, comparative studies of how cybersecurity governance models are realized in sectors and how multi-framework alignments have been made in practice, especially in the U.S. context where NIST-led guidance takes center stage in addition to global standards and sectoral regulation. The gap that this paper fills is the comparative analysis of cybersecurity governance in five sectors, namely, financial services, healthcare, energy and OT, local government, and higher education. The paper looks at the structure of governance responsibilities (boards, executive management, risk and compliance functions) and how organizations integrating and customizing frameworks (NIST CSF, ISO/IEC 27001, COBIT 2019, COSO, ITIL) and how new AI-driven practices are starting to transform governance. It is hoped that these cross-sector trends, divergences and lessons will help to guide boards, regulators and practitioners aiming to enhance cybersecurity governance within the U.S. industries without sacrificing global best practice.

2. CONCEPTUAL AND REGULATORY BACKGROUND

The sphere of cybersecurity governance does not exist in isolation but is integrated with more corporate, IT and risk-governance structures and is indisputably framed by an elite number of influential frameworks and regulatory demands. That landscape is explained in this chapter. It initially places the governance of cybersecurity in the context of the current governance theory and the board-level functions, and thereafter provides a summary of the roles, processes and performance structure of cross-industry frameworks like NIST CSF, ISO/IEC 27001 and COBIT 2019 (NIST, 2024; Essien et al., 2022; Reuben-Owoh and Haig, 2025). It then looks at multi-actor and sectoral tools, such as the ISO/IEC 27032, the DCAF guide, the NCSS model offered by ENISA and the World Bank Sectoral Cybersecurity Maturity Model, which supersedes the governance of single organizations (DCAF, 2021; Sarri et al., 2023; World Bank et al., 2023). The chapter ends with the connection of these concepts to the U.S. regulatory environment and integrated ERM perspectives which form the basis of the further sector analysis.

2.1 Cybersecurity in corporate and risk governance

Modern practices are moving the area of cybersecurity to the center of corporate, IT and risk control. World Economic Forum and NACD board-level documents highlight that cyber risk is one of the leading enterprise risks and needs to be toned at the top level in a well-organized manner and integrated into strategy and risk appetite (World Economic Forum, 2021). Empirical research on board practice demonstrates that information asymmetries, absence of expertise and fragmented reporting tend to compromise attention to cyber risk and create discrepancies between formal responsibility and effective oversight (Proudfoot et al., 2023; Gale et al., 2022).

2.2 Cross industry structures and matching

NIST CSF 2.0 institutionalises governance as one of the essential functions of Identify, Protect, Detect, Respond and Recover. The new GOVERN functionality dictates that the organizational cybersecurity risk management strategy, expectations and policy are defined, disseminated and tracked, and splits this up into organizational context, risk strategy, role and responsibility, and oversight (NIST, 2024). This outcome-focused approach is supplemented with ISO/IEC 27001, which offers a certifiable information security management system (ISMS) that integrates information security into organizational strategy and processes via risk assessment, selection and ongoing

SJIF Impact Factor (2026): 8.863| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 11 | Issue: 3 | March 2026 - Peer Reviewed Journal

improvement of controls (ISO, 2022; Peters, 2025). Unlike NIST CSF, the ISO/IEC 27001 complies with documented policies, roles and procedures, underpinned by internal audit and management review as the means to entrench governance.

The framework of governance and management of enterprise IT in COBIT 2019 is wider and more concerned with the creation of value, risk reduction, and resource optimization (Adams, 2024). Its model separates governance goals (e.g. benefits delivery, risk optimization), management goals (plan, build, run, monitor) and relates both to processes, goals and metrics. The Three Lines Model reflects this governance-management boundary, and it provides operational management, risk and compliance, and internal audit responsibilities but acknowledges that organizations occasionally cross lines to achieve efficiency (Bongiovanni et al., 2024).

Systematic reviews give evidence-based perspective of how these tools, in their organization, organize practice. A major review identifies twelve well-known frameworks and seventeen standards, anoints ISO/IEC 27001 and NIST CSF as the most influential, and sector-specific standards like ISA/IEC 26443 and technical ones like SCAP (Reuben-Owoh & Haig, 2025). Alignment work illustrates how organizations can optimize cyber risk governance by considering NIST, ISO and COBIT as complementary and interlocking inputs as opposed to competing options (Essien et al., 2022).

2.3 Instruments of multi-actor and sectoral governance

Several tools are specifically related to governance in multi-actor environments. The ISO/IEC 27032 is concerned with collaboration and alignment of internal teams, external partners, governments and users, and encourages the stakeholders to work together to create a sustainable digital ecosystem (PECB, 2025; DataGuard, 2024; Ankit, 2025). The DCAF Guide to Good Governance in Cybersecurity incorporates cyber policy into the overall governance in the security sector, with accountability, transparency and rule of law playing a crucial role in how states and non-state actors discuss cyberspace (DCAF, 2021).

At the national and sectoral level, the governance framework of national cybersecurity strategies (NCSS) of ENISA describes political, strategic, operational and technical functionalities, coupled with leadership, co-ordination, stakeholder engagement and performance monitoring (Sarri et al., 2023). Even though this architecture was created to be applicable to EU member states, it is applicable to multi-agency or public-private partnerships in the United States. World Bank Sectoral Cybersecurity Maturity Model (SCMM) introduces another dimension of maturity assessment at a sector level by evaluating the maturity through such dimensions as Cybersecurity Governance, Cyber Risk Management, Cybersecurity Measures, Cyber Capacity Building and Incident Response and Crisis Management (World Bank et al., 2023; Teknowledge, 2025). The SCMM considers every critical sector to be a system whereby the interdependency between regulators and operators with external stakeholders defines resilience.

2.4 Sector-specific conceptual work

Sectoral reviews also narrow governance concepts as well as bring out the situational needs. In the case of higher education institutions (HEIs), useful cybersecurity frameworks should be both extensive but flexible to open networks, multi-user base, and decentralization of decision-making. The policies, awareness and training, incident response, access control and continuous improvement, and recurring components are common and need to be adjusted to the institutional structure and culture (Barruga, 2025; Barruga and Palaoag, 2025). Municipal cybersecurity is also categorized as governance, risk management, technology, people and external environment in local government studies and outlines recurring areas of failure: inadequate governance mechanisms, no specific leadership, and unreliable funding with increasing dependence on digital matters (Hossain et al., 2024, 2025).

New work associates AI and sustainability with cybersecurity governance. Various threat-modelling approaches can be assisted by LLM to identify assets and threat and attack-paths automation, which may reinforce the risk assessment and decision support process, but may also develop new conditions on data quality, model disclosure and energy consumption (Jersic et al., 2025). A complementary strand suggests the frameworks of governance that combine blockchain, AI and legal foundations, ensuring the enforcement of policies, compliance evidence, as well as acceptable cyber risk (Toapanta et al., 2025).

2.5 U.S. regulatory environment and holistic thinking.

The strands of these concepts are interlaced with a developing regulatory landscape in the U.S. NIST CSF 2.0, which is an appeal to the industry, government agencies, and other organizations, has been incorporated into the list of references of many regulators and sector profiles (NIST, 2024). Financial services, healthcare, energy and public sector organizations and practitioners are seen to define regulatory requirements in the context of governance and transitioning to enterprise-wide risk and resilience outside of a limited IT security perspective (KPMG, 2024, 2025). Empirical accounting research indicates that regulators and shareholders are placing increased emphasis on firms' cybersecurity risk management disclosures in Form 10-K filings, including board oversight, management responsibilities, and board-level involvement (Gao and Calderon, 2025).

SJIF Impact Factor (2026): 8.863| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 11 | Issue: 3 | March 2026 - Peer Reviewed Journal

The integrated perspectives propose the inclusion of cybersecurity governance within enterprise risk management (ERM) and alignment of strategic, tactical and operational aspects through a coherent model (Oh et al., 2025). Guidance by practitioners also recommends a comprehensive approach where boards, CISOs and risk leaders adopt a cross-cutting governance approach, rather than a technical siloed role in cybersecurity (Miller, 2024). These sources offer the conceptual and regulatory framework of the comparative sectoral analysis which ensues.

3. THE U.S. SECTORAL CYBERSECURITY GOVERNANCE MODELS

This section describes the structure of cybersecurity governance in five areas in the U.S., financial services, healthcare, energy and OT, local government, and higher education. In both instances, governance is an expression of cross-industry structures, sector-based regulation and directions, and organizational realities outlined in recent literature.

3.1. Financial services and banking

Cybersecurity governance, in the financial services industry, is closely intertwined with regulatory focus and systemic-risk issues. The comparative analyses detail dense regimes of data protection, incident response and risk management, which are becoming increasingly aligned in general expectations of how they should be governed, despite still existing differences in breach notification and privacy regulations (Uzougbo et al., 2024).

In organizations, cybersecurity governance typically centers on the CISO, who is responsible for developing and implementing policies, coordinating with legal, compliance, risk, and audit functions, and aligning cybersecurity practices with established standards such as ISO/IEC 27001 (Almohri, 2024). The cybersecurity program is managed by board-level or required risk committees that are aided by management-level committees and three-lines-of-defense model that distinguishes operations, risk/compliance and internal audit, whereby a lack of control and regulatory non-conformity is greater when there is a lack of distinction between the three lines (Akinsulire and Ohakawa, 2024).

The adoption of a framework is closely tied to the NIST CSF and tends to be consistent with the ISO and a sector specific profile. The Financial Services Sector Cybersecurity Profile, which is explicitly found on NIST CSF, is a harmonization of thousands of regulatory statements into fewer diagnostic objectives and has been identified as a comprehensive instantiation of the Framework to financial services (Cyber Risk Institute, 2025). Consequently, NIST categories and subcategories are often discussed in terms of governance, and Profile provides a common language to boards and regulators.

CISOs operate under sustained pressure from organizational leadership, regulators, and data-protection regimes to demonstrate compliance and resilience against cyber threats (KPMG, 2024; Schwab, 2025). Further investigations into industry cyber threats support discussions of governance frameworks capable of addressing strategic challenges beyond technical control-level issues (Alademehin, 2025). Collectively, the sector has developed governance structures characterized by clearly defined board and CISO roles, formal risk management processes, alignment with multiple frameworks, and a strong compliance orientation.

3.2 Healthcare organizations

Patient-sensitive data, life-critical services and chronic resource limitations are the other combination of drivers in healthcare organizations. According to global surveys, cybersecurity has become a top topic on the agenda of most boards, but a major lack exists in the resources available, preparation and systematic risk evaluation during incidents (O'Brien et al., 2020). There is an array of concerns about manipulation or loss of electronic health records, service disruption and undermined trust, making the governance of cybersecurity directly connected to clinical safety and organizational reputation.

Recent research about the digital transformation of healthcare suggests connected models that relate governance, employee behavior and technology. Proper governance should encompass both technical planning (access controls, monitoring), and behavioral aspects (awareness, perceived vulnerability, deterrence) based on frameworks like ISO/IEC 27001 and NIST as highly structured templates adapted to the clinical environment (Alharbi and Alkhalifah, 2025).

Critical analyses of the state of cybersecurity in healthcare reveal increasing adoption of sophisticated technologies such as encryption, identity and access control, intrusion detection, and, in some cases, blockchain; however, technical controls alone are insufficient without corresponding attention to human factors, third-party risk, and organizational processes (Javid et al., 2023). Compliance wise, HIPAA and other rules tend to push risk forward, and risk is defined more or less along the lines of control compliance. According to auditing work, this form of compliance-based work is often inflexible and biased, and suggests complementing it with dynamic methods, including red-team/blue-team exercises (Itani et al., 2024). Similar observations are made by the practitioner reports, which indicate that

SJIF Impact Factor (2026): 8.863| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 11 | Issue: 3 | March 2026 - Peer Reviewed Journal

compliance is required but not adequate; the governance must be more focused on resilience, incident response preparedness, readiness and workforce awareness (KPMG, 2025).

In general, the formal basis of healthcare governance lies in the regulation of privacy and security and in general structures, yet operational issues of complex systems, behavior of workforce and finite resources confront governance. Governance should, therefore, handle close couplings among patient safety, digital transformation, and staff compliance and ensure it is in line with the U.S. standards and international frameworks.

3.3 Energy, utilities and industrial/OT setups

In the energy and utilities sector, cybersecurity governance is inseparable from the safety, reliability, and protection of critical infrastructure. Guidance on OT cybersecurity from the U.S. Department of Energy highlights that programmable devices such as industrial control systems and building management systems introduce cyber risks, including configuration errors and malicious manipulation, that can result in harmful physical outcomes (DOE, 2025). Organizations are also called to know their OT posture, establish the tolerable level of risks and incorporate OT cybersecurity within wider governance frameworks instead of seeing it as a technical sidenote (DOE, 2025).

The SCMM provides a sector-level perspective by evaluating how national authorities, regulators, and sector participants coordinate roles, responsibilities, and oversight, emphasizing that every vital sector must be understood as a system of interdependencies among actors (World Bank et al., 2023). In the case of the U.S. energy and utilities sector, this perspective aligns with governance structures that include federal agencies, independent system operators, state regulators, and other asset owners.

According to practitioner advice, energy CISOs are likely to become strategic collaborators in the management of OT risk, regulatory compliance and decarbonization-driven digitalization, the integration of NIST-style risk management with industry standards and safety-critical engineering activities (KPMG, 2025; Teknowledge, 2025). Analysis of Sectoral GRC defines manufacturing and energy companies as having significantly a specific problem with IT-OT convergence and the necessity to harmonize cyber- safety and operational risk management (Schwab, 2025). Governance can therefore work at two levels; internally organizations need to empower security leaders to affect the operations; and externally sector-level governance needs to facilitate coordination of guidance, incentives and oversight.

3.4 Local governments and the public sector

The United States local and public agencies are growing more reliant on digital services and tend to have limited resources and divided governments. Systematic review-based conceptual frameworks emphasize governance, risk management, technology, people and external environment as essential elements of municipal cybersecurity and point out that proper governance needs clear leadership and routine roles, cross-departmental coordination and sustainable funding, rather than policy documents alone (Hossain et al., 2024).

A document reviews the problems: current system, inadequate knowledge, constrained resources and complicated intergovernmental linkages, which forms a mismatch between the threats and the governance ability (Hossain et al., 2025).

Governance models including the NCSS model of ENISA and the DCAF guidelines offer reference schemes at the national and regional levels that are built on the principles of multi-level coordination, stakeholder involvement, and democratic responsibility (Sarri et al., 2023; DCAF, 2021). Practitioner reports highlight that CISOs in the public sector are so stretched by the combined pressures of increasing attacks and inadequate resources that they demand new governance models to embed cyber into a broader societal perception of risk and performance management and to draw more on shared services and external partners (KPMG, 2025; Schwab, 2025).

The governance of cybersecurity to local and public entities in the United States is hence typified by high expectations of norms and growing reliance on national frameworks, yet unequal implementation ability and absence of sector-specific frameworks that are analogous to finance or energy.

3.5 Research and Learning Establishments

Colleges and universities have IT environments that are open, large and heterogeneous, sensitive to personal and research data, and the governance cultures of these institutions are often decentralized. The systematic review research demonstrates that HEIs have generally been based on a combination of general frameworks (ISO/IEC 27001, NIST CSF) and sector-specific guidelines, which in turn should be adapted to academic standards, including open access, federated identity and shared governance (Barruga, 2025).

SJIF Impact Factor (2026): 8.863| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 11 | Issue: 3 | March 2026 - Peer Reviewed Journal

The most common elements of frameworks are policies, risk assessment, access control, incident response, awareness and training and continuous improvement, yet the resource-intensive aspect and the heterogeneous nature of the user base, as well as the inability to integrate cybersecurity into institutional planning and quality assurance, hinder its implementation (Barruga, 2025). Other research proposes that colleges are also becoming more interested in maintaining academic autonomy as they move to centralize some security functions (identity management, network monitoring) and leave others to faculties or departments (Barruga & Palaoag, 2025).

These industry lessons echo cross-industry surveys that suggest ISO/IEC 27001 and NIST CSF as a standard framework, which is understood through organizational context (Essien et al., 2022; Reuben-Owoh & Haig, 2025). Context in HEIs involves freedom of academic research, sharing of research and responsibilities related to federal funding and data privacy. Forms of governance are thus inclined to centralize committees or councils which control the cybersecurity policy with the decentralized roles in faculties and research units.

4. COMPARATIVE ANALYSIS ACROSS INDUSTRIES

The sectoral mapping indicates that U.S. industries are attracted to parallel setups but transform them into other forms of governance. The four dimensions of the comparison between such arrangements are (i) board and executive oversight; (ii) formalization and centralization; (iii) regulatory and institutional pressure; and (iv) framework alignment, risk oversight and technological enablers.

4.1 Board and executive control

In most industries, however, cybersecurity is being treated as a board level issue, though the intensity and regularity of supervision do not always exist. The principles introduced at the board level highlight the importance of explicit distribution of cyber-risk management, awareness of the economic effects and embedding them in the risk management strategy and risk appetite (World Economic Forum, 2021). Large energy companies and financial institutions are more likely to make approximations to this model, with formal risk committees and empowered CISOs with supporting three-lines-of-defense constructs (Almohri, 2024; Akinsulire and Ohakawa, 2024; DOE, 2025). According to reports by healthcare surveys, cybersecurity has become a frequent topic on the leadership agenda but points out inconsistencies in rhetorical commitment and long-term investment (O'Brien et al., 2020; KPMG, 2025). Responsibilities in local government and higher education institutions are often disconnected, and informal reporting and conflicting priorities prevent the practice of formal accountability applying to practice (Hossain et al., 2024, 2025; Barruga, 2025).

4.2 Formalization, centralization and regulatory pressure

Finance services and energy/OT have more formal and centralized governance, and codified roles, lines of escalation, policy frameworks in line with the supervisory requirements and industry standards (Almohri, 2024; DOE, 2025; World Bank et al., 2023; KPMG, 2024). The intensity of regulation is strong: voluntary standards like ISO/IEC 27001 and NIST CSF are intertwined with binding requirements and form a web of commitments that governance entails (Reuben-Owoh and Haig, 2025; Uzougbo et al., 2024).

Important although more limited regimes apply to healthcare and higher education (e.g., HIPAA, FERPA, conditions in research-funding), with a larger amount of discretion (and hence variability) in the organizing of governance (Barruga, 2025; Javaid et al., 2023). Local jurisdictions can have the laxest cyber-specific requirements without having to comply with general data-protection and public-records legislation; this further widens the discrepancies between anticipated and realistic governance (Hossain et al., 2024, 2025).

4.3 Architectural congruence, risk management and enabling technology

Organizations in various industries are likely to use few frameworks but use them differently. According to reviews, NIST CSF and ISO/IEC 27001 are always the most visible with COBIT 2019 and other IT governance models being auxiliary (Reuben-Owoh and Haig, 2025; Essien et al., 2022; Fandom, 2025). Multi-framework alignment is best operationalized by financial institutions, especially those that have the NIST financial services profile which aligns regulatory requirements with CSF outcomes (KPMG, 2024; Cyber Risk Institute, 2025). OT and energy organizations are matching the standards of NIST and ISA/IEC to the DOE and other guidance (DOE, 2025; World Bank et al., 2023; Teknowledge, 2025).

In fact, HEIs and local governments usually selectively assume one or two frameworks, and more sometimes concentrate on the aspects of awareness and policy without developing more complex forms of governance and metrics (Barruga, 2025; Hossain et al., 2024, 2025). In industries, the adoption of integrated GRC platforms and ongoing monitoring continues to complicate the growth of those mature organizations, yet the capabilities are still uneven and resource-based (Schwab, 2025). Threat modelling with AI provides a possible enhancement of risk analysis by facilitating various approaches with the help of LLMs, but it also raises new governance challenges of transparency, data quality and energy usage (Jersic et al., 2025). In the case of smaller, under-resourced organizations, they are only

SJIF Impact Factor (2026): 8.863| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 11 | Issue: 3 | March 2026 - Peer Reviewed Journal

aspirational; the governance is based primarily on policies, simple risk registers and regular audits (Barruga, 2025; Hossain et al., 2024, 2025).

4.4 Convergence and divergence

There are three convergence patterns that can be distinguished. To begin with, it is widely accepted that the problem of cybersecurity governance is not a technical problem but an enterprise-wide one (World Economic Forum, 2021; Essien et al., 2022; Reuben-Owoh and Haig, 2025; World Bank et al., 2023). Second, cross-industry frameworks are solidified into a de facto foundation with NIST CSF, ISO/IEC 27001 and COBIT 2019 establishing a shared base across the sectors (Essien et al., 2022; Reuben-Owoh and Haig, 2025; Fandom, 2025). Third, governance, risk, and compliance (GRC) logic coordinates decision rights, risk identification, and compliance requirements, and is widely recognized as foundational to organizational resilience (Schwab, 2025; World Bank et al., 2023).

Simultaneously, differences are high. These differences are drastic in regulatory intensity and compliance posture across highly and under-regulated sectors (finance, energy/OT) and local government, most higher education institutions. Confidentiality-focused banking, safety-focused energy/OT, clinically focused healthcare and openness-oriented HEIs and municipalities are risk-profiles that differ between each other (Alademehin, 2025; Javaid et al., 2023; Teknowledge, 2025; Hossain et al., 2024, 2025). Further distinctions between sectors are the capacity and culture of the organization: big financial and energy companies have the ability to sustain teams of specialists, independent audit and sophisticated GRC tooling, and local governments and HEIs usually have small teams with multiple roles (Almohri, 2024; KPMG, 2024; World Bank et al., 2023; Barruga, 2025; Hossain et al., 2024, 2025). Lastly, at present, only a small fraction of organizations can test the AI-enabled tools of governance (Jersic et al., 2025; KPMG, 2024).

5. DISCUSSION AND IMPLICATIONS

The comparative analysis suggests that the U.S. industries are coming towards a common conceptualized toolkit of cybersecurity governance which is constructed based on NIST CSF, ISO/IEC 27001, COBIT 2019 and GRC thought but is diverged in terms of their levels of implementation and standards. It has been demonstrated through framework alignment work that a coordinated usage of these tools could provide a comprehensive and versatile foundation of cyber risk governance, transforming cybersecurity into a fundamental part of enterprise governance and ERM (Essien et al., 2022; Oh et al., 2025; Miller, 2024). It is systematic reviews that affirm that organizations that cut across sectors tend to drift to this small set of frameworks regardless of the degree of adoption and combinations (Reuben-Owoh & Haig, 2025).

Simultaneously, sectoral literature, particularly local government and higher education, illustrates that there is no evidence to suggest that governance theory and guidance in relation to structure make assumptions of institutional capacity that many organizations do not have. Constant mismatches between dangers and assets, command and skill underscore the danger that formal governance frameworks are little considerably more than symbolic (Hossain et al., 2024, 2025; Barruga, 2025).

The AI-based threat modelling implies that the governance environment is returning. The tools built on LLM can enhance the accessibility and reproducibility of risk assessment but pose new governance-related questions regarding the model oversight, transparency and sustainability (Jersic et al., 2025; Toapanta et al., 2025). Boards and regulators will be required not only to oversee security controls and governance structures, but also to ensure appropriate oversight of the tools and methodologies used in system design and risk assessment.

As a board member and an executive leader, the primary implication attracted by the report is that cybersecurity governance cannot be narrowed down to checklists or be left solely in the hands of technical experts. Good governance means that responsibility at a committee level, regular decision-relevant reporting to the CISOs, integrating cyber risk into the strategy and risk appetite, and actively monitoring the use of the frameworks and tools are not merely embraced in words (World Economic Forum, 2021; Gao and Calderon, 2025).

The findings suggest harmonization and support to requirements instead of proliferation to the requirements by policymakers and regulators. Profiles or mappings of NIST CSF, ISO/IEC 27001 and other frameworks can be used as sectoral obligations, e.g., financial services and are represented in national code-to-principal mappings (KPMG, 2024; DSIT, 2025). Maturity models of governance may be used to determine the areas of under-investment that require direct investment (funding), common services or template policies (World Bank et al., 2023; Hossain et al., 2024, 2025). There should also be anticipatory guidance on AI-enabled security devices, so that they can improve accountability and not blur it (Jersic et al., 2025).

SJIF Impact Factor (2026): 8.863| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 11 | Issue: 3 | March 2026 - Peer Reviewed Journal

6. SUGGESTIONS AND INTEGRATIVE GOVERNANCE REFERENCE MODEL

The comparative analysis shows convergence and fragmentation in the way U.S. industries regulate cybersecurity: the organizations are likely to use similar frameworks, but their regulatory force, capacity and risk profile are significantly different (Essien et al., 2022; Reuben-Owoh and Haig, 2025; Hossain et al., 2024, 2025; Barruga, 2025). This section transforms such findings into guide and a brief reference model. It initially provides cross-sectoral suggestions to boards, executives and risk leaders on how to formalize oversight and harmonize the frameworks and tailor governance to the sector, such as AI-based security tools (World Economic Forum, 2021; Jersic et al., 2025). It then makes implications to regulators and standard-setters and synthesizes an integrative three-layer model of governance, capable of being reconfigured to different sectors, keeping in line with NIST CSF, ISO/IEC 27001 and COBIT 2019 (NIST, 2024; Oh et al., 2025; World Bank et al., 2023).

6.1 Inter-industry guidelines for organizations.

Institutionalize cyber as a requirement of the board.

Designate specific cyber-risk responsibility to a suitable committee, demand frequent decision-oriented reporting of the CISO and tie cyber risk to strategy and risk appetite (World Economic Forum, 2021; Gao and Calderon, 2025).

Align, and not accumulate frameworks

Regard ISO/IEC 27001, NIST CSF (with the GOVERN function of 2.0) and COBIT 2019 as hierarchical elements, that is, ISMS discipline, outcome-based risk management and IT governance, instead of competing standards (Essien et al., 2022; Reuben-Owoh and Haig, 2025).

Integrate cyber into three lines structures

Assign cybersecurity roles within the operational management, risk/compliance and internal audit, and tailor the Three Lines Model and the governance-management difference of COBIT to organizational scale and capacity (Bongiovanni et al., 2024; Essien et al., 2022).

Operate with a standard backbone, sector specific

Use NIST/ISO/COBIT as a common reference point and policy, roles and metrics to highly sector-specific risk profiles and institutional realities, e.g. political supervision and resource constraints in local government, or openness and academic freedom in HEIs (Hossain et al., 2024, 2025; Barruga, 2025; Jersic et al., 2025).

Process and AI tooling, people, and process as subjects of governance

Identify capacity, culture and standard process discipline (access management, incident handling) as shared limitations, and make training, culture and AI-based security tools subject to conscious control and strict accountability and monitoring (Hossain et al., 2024, 2025; Jersic et al., 2025).

6.2 Regulators and standard setters' recommendations.

Co-ordinate well-established structures

Repurpose existing alignment efforts instead of creating new and distinct models to express sectoral requirements in mappings or profiles of NIST CSF, ISO/IEC 27001 and other standards (Reuben-Owoh, Haig, 2025).

The sectors that are support capacity constrained.

Eliminate local government and education resourcing and expertise shortages using shared services, minimum control catalogues, and funding associated with governance maturity, as well as new mandates (Hossain et al., 2024, 2025; World Bank et al., 2023).

Predict AI-driven security in directions and monitoring.

Asking questions about transparency, validating and humanizing LLM-based threat modelling and the like to make sure that AI reinforces, and not hides, accountability (Jersic et al., 2025; Toapanta et al., 2025).

6.3 Integrative cybersecurity governance reference model

In the case of the cybersecurity governance across the U.S. industries, the integrative reference model can be summarized into three layers:

Strategic governance at the board and executive level: establishes cyber-risk appetite, aligns frameworks such as NIST CSF, ISO/IEC 27001, and COBIT 2019, and embeds cybersecurity within corporate or mission strategy. It also ensures clear oversight structures and reporting lines that demonstrate board-level direction (World Economic Forum, 2021; Essien et al., 2022).

SJIF Impact Factor (2026): 8.863| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 11 | Issue: 3 | March 2026 - Peer Reviewed Journal

Translational governance (CISO, risk, compliance, architecture): translates strategy into policies, sets targets at maturity levels and sectoral profiles, aligns the three lines, keeps regulatory-to-framework mappings, and regulates advanced tooling, such as AI-enabled risk analysis (Essien et al., 2022; Jersic et al., 2025; Oh et al., 2025).

Operational implementation and learning (IT/OT, business units, local entities): engages operational controls and incidence response, propels operational data and other learning realized at operations into higher levels, and cooperates with other operational entities and public (especially in multi-actor sectors like local governments and critical infrastructure, where sector-level frameworks and partnership are necessary) (World Bank et al., 2023; Hossain et al., 2024, 2025; Teknowledge, 2025; DSIT, 2025).

The model does not propose a particular organizational chart but determines governance functions that must be seen, in one way or another, in sectors. It provides a generalized prism through which to contrast and refine governance of cybersecurity and provides a basis through which empirical future research can be structured.

7. LIMITATIONS AND FUTURE RESEARCH

This research is a desk-based, integrative analysis that synthesizes the usual frameworks, sectoral frameworks and empirical reviews, as opposed to gathering primary data. The image of hegemonic schemes and alignment patterns is thus defined by the focus of academic and professional discourse already taking place (Essien et al., 2022; Reuben-Owoh and Haig, 2025).

The emphasis on the U.S. industry and five segments, financial services, healthcare, energy/OT, local government and higher education, implies that such other areas (e.g. tech platforms, small manufacturing) and organizational types (e.g. small privately owned firm) are not explicitly studied. Sectoral instruments like the SCMM have been used so far in selected areas and nations, which makes it difficult to generalize (World Bank et al., 2023).

The AI-based cybersecurity governance is not yet fully treated. Existing research on LLM-based threat modelling and built-in blockchain-AI-lawful systems remains preliminary, and the influence on the board practice, regulation and sectoral maturity are yet to become clear (Jersic et al., 2025; Toapanta et al., 2025).

Future studies should, therefore:

1. Carry out empirical studies (surveys, case studies), which are sector-specific, to verify the consistency of the proposed governance model with practice.
2. Carry out comparative international studies of the U.S. models relative to other regulatory frameworks utilizing alignment logic and framework rankings to provide common reference points.
3. Transform conceptual frameworks of local government and higher education into measurement tools that can monitor improvement over time in governance (Hossain et al., 2024, 2025; Barruga, 2025).
4. Establish a specific research agenda on AI-enabled governance tools, how boards, CISOs and regulators assess, approve and oversee such tools and their interaction with the existing frameworks, including NIST CSF and ISO/IEC 27001.

8. CONCLUSION

The paper investigated the ways of implementing cybersecurity governance model in the key industries in the U.S. through the synthesis of global models, sector maturity models, and empirical reviews. It was revealed that organizations are aligning ISO/IEC 27001, NIST CSF and COBIT 2019 more frequently to create layered cyber risk governance ecosystems instead of single standards. Comparisons of local government, higher education, healthcare and finance and energy sectors indicated that there were continually higher levels of disparity in formalization, capacity and regulatory pressure, with under-resourced sectors of public and education languishing behind. The next feature is the growth of AI-powered threat modelling which only confirms the necessity to regulate security controls, as well as the tools that influence risk decision making. All the above findings help to support an integrative reference model that is framework-sensitive and adjustable to new technologies.

REFERENCE

1. *Adams, N.R. (2024). COBIT 2019: IT governance framework. https://itlawco.com/cobit-2019-it-governance-framework/*
2. *Akinsulire, A. A., & Ohakawa, T. C. (2024). Enhancing Cybersecurity Governance in Financial Institutions: A Quantitative Study on Control Deficiencies and Regulatory Compliance (2024).*
3. *Alademehin, A. (2025). Top 5 Cyber security Risks for Financial Institutions in 2025: Case Studies and Strategic Mitigation. Available at SSRN 5267663.*

4. *Alharbi, A. & Alkhalifah, A. (2025). Cybersecurity governance in the healthcare sector during digital transformation: an integrated model and hybrid analytical approach. Frontiers in Public Health. 13. 10.3389/fpubh.2025.1703689.*
5. *Almohri. H,. (2024). Governance of Cybersecurity in Banking and Financial Organizations. Facts and trends of how cybersecurity is governed within organizational structures in the banking/financial sectors (GCC and global perspectives). kibs.edu.kw/wp-content/uploads/2025/02/Research-Final-Approved-Governance-of-Cybersecurity-in-Banking-Jan-2025.pdf*
6. *Ankit, S. (2025). ISO 27032 Stakeholder Collaboration for effective Cybersecurity Governance. https://www.neumetric.com/journal/iso-27032-stakeholder-collaboration-2972/*
7. *Barruga, M. B. (2025). SYSTEMATIC REVIEW OF CYBERSECURITY FRAMEWORKS FOR HIGHER EDUCATION INSTITUTIONS: CHARACTERISTICS, COMPONENTS, AND CHALLENGES. International Journal of Applied Mathematics, 38(4s).*
8. *Barruga, M., & **Palaoag, T.** (2025). Cybersecurity Strategy for Higher Education Institutions: A Thematic Analysis on Standards and Frameworks. Journal of Information Systems Engineering and Management. 10. 1140-1152. 10.52783/jisem.v10i43s.8533.*
9. *Bongiovanni, I., Slapničar, S., Axelsen, M., & Stockdale, D. (2024). The Three Lines Model in Cybersecurity Governance and Risk Management. ISACA Journal, 1(2024).*
10. *Cyber Risk Institute. (2025). Our Cyber Profile for the financial sector is a global standard for cyber risk assessment. https://cyberriskinstitute.org/the-profile/*
11. *DataGaurd. (2024). ISO 27032: Guidelines for cybersecurity management. https://www.dataguard.com/blog/iso-27032/*
12. *DCAF. (2021). Guide to Good Governance in Cybersecurity. dcaf.ch/sites/default/files/publications/documents/CyberSecurity_Governance_EN_Jan2022.pdf*
13. *DOE (2025). Energy and Cybersecurity Integration. https://www.energy.gov/femp/energy-and-cybersecurity-integration*
14. *DOE. (2025) Operational Technology Cybersecurity for Energy Systems. https://www.energy.gov/femp/operational-technology-cybersecurity-energy-systems*
15. *DSIT. (2025). Mapping cyber governance code to WEF principles for Board Governance of Cyber Risk. https://www.gov.uk/government/publications/cyber-governance-mapping/mapping-cyber-governance-code-to-wef-principles-for-board-governance-of-cyber-risk*
16. *Ekpo, K. " A Literature Review of Secure Digital Transformation Practices in Regulated Sectors " Sarcouncil Journal of Engineering and Computer Sciences 5.3 (2026): pp 1-14.*
17. *Essien, I. A., Cadet, E., Ajayi, J. O., Erigh, E. D., Obuse, E., Ayanbode, N., & Babatunde, L. A. (2022). Optimizing cyber risk governance using global frameworks: ISO, NIST, and COBIT alignment. Journal of Frontiers in Multidisciplinary Research, 3(1), 618-629.*
18. *Fandom. (2025). Top 10 Cybersecurity Frameworks to Know in 2025. https://faddom.com/top-10-cybersecurity-frameworks-to-know-in-2025/*
19. *Gale, M., Bongiovanni, I., & Slapnicar, S. (2022). Governing cybersecurity from the boardroom: challenges, drivers, and ways ahead. Computers & Security, 121, 102840.*
20. *Gao, L., & Calderon, T. G. (2025). Cybersecurity risk governance and companies' cybersecurity risk disclosures in their 10-K filings. Journal of Accounting and Public Policy, 54, 107376.*
21. *Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2024). Local government cybersecurity landscape: A systematic review and conceptual framework. Applied Sciences, 14(13), 5501.*
22. *Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2025). Cybersecurity in local governments: A systematic review and framework of key challenges. Urban Governance.*
23. *ISO. (2022). ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection - Information security management systems - Requirements*
24. *Itani, D., Itani, R., Eltweri, A. A., Faccia, A., & Wanganoo, L. (2024, February). Enhancing cybersecurity through compliance and auditing: a strategic approach to resilience. In 2024 2nd international conference on cyber resilience (ICCR) (pp. 1-10). IEEE.*
25. *Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2023). Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. Cyber Security and Applications, 1, 100016.*
26. *Jeršič, N., Turkanović, M., & Beranič, T. (2025). Towards a Sustainable Cybersecurity Governance: Threat Modelling with Large Language Models. Sustainability, 17(23), 10569.*
27. *KPMG. (2024). Cybersecurity considerations 2024: Financial services sector.*
28. *KPMG. (2025). Cybersecurity considerations 2025. https://kpmg.com/xx/en/our-insights/ai-and-technology/cybersecurity-considerations-2025.html*
29. *Miller, M. (2024). Rethinking Cybersecurity Governance: A Comprehensive Approach for CISOs. https://auditboard.com/blog/rethink-cybersecurity-governance-a-comprehensive-approach*
30. *Navigating uncertainty and embracing innovation. https://kpmg.com/xx/en/our-insights/ai-and-technology/cybersecurity-considerations-2024-financial-services-sector.html*
31. *NIST, (2024). The NIST Cybersecurity Framework (CSF) 2.0. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf*
32. *O'Brien, N., Martin, G., Grass, E., Durkin, M., Darzi, A., & Ghafur, S. (2020). Cybersecurity in healthcare: Comparing cybersecurity maturity and experiences across global healthcare organizations. Available at SSRN 3688885.*

SJIF Impact Factor (2026): 8.863| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 11 | Issue: 3 | March 2026 - Peer Reviewed Journal

33. *Oh, K. B., Hoang, G., Sturdy, J., & Guo, S. S. (2025). Integrated Cybersecurity Governance and ERM Framework. In Cybersecurity Governance: An Enterprise Risk Management Strategy for Cyber Risk Control (pp. 89-112). Singapore: Springer Nature Singapore.*
34. *PECB. (2025). Guidelines to Cybersecurity with ISO 27032. https://pecb.com/en/article/guidelines-to-cyber-security-with-iso-27032*
35. *Peters, S. (2025). The Ultimate Guide to ISO 27001. https://www.isms.online/iso-27001/*
36. *Proudfoot, J. G., Cram, W. A., Madnick, S., & Coden, M. (2023). The Importance of Board Member Actions for Cybersecurity Governance and Risk Management. risk, 1, 2.*
37. *Reuben-Owoh, B., & Haig, E. (2025). A Systematic Review of Voluntary Cybersecurity Standards and Frameworks: B. Reuben-Owoh, E. Haig. International Journal of Information Security, 24(5), 206.*
38. *Sarri, A., Bascuñana, G.F., Gross, A.K., Chiarelli, F., & Preasca, M. (2023). A Governance Framework for National Cybersecurity Strategies. ENISA. https://www.enisa.europa.eu/sites/default/files/publications/A%20Governance%20Framework%20National%20Cybersecurity%20%20Strategies.pdf*
39. *Schwab, W. (2025). Part 4: GRC in Context: How Cybersecurity Governance, Risk, and Compliance Varies by Industry. https://sitsi.pacanalyst.com/part-4-grc-in-context-how-cybersecurity-governance-risk-and-compliance-varies-by-industry/*
40. *Teknowledge. (2025). The Imperative of Collective Defense: The Emergence of Sectoral SOCs. https://teknowledge.com/insights/the-imperative-of-collective-defense-the-emergence-of-sectoral-socs/*
41. *Toapanta T, M., Buenaño, J. J., Vayas C, S., Nogales, P, R., Del Pozo D, R., Orizaga T, A., & Andrade A, D. (2025). Perspectives on a Cybersecurity Governance Framework Integrating Blockchain, Artificial Intelligence, and Legal Base for one Organization. Journal of Posthumanism, 5(5), 2701–2718. https://doi.org/10.63332/joph.v5i5.1664*
42. *Uzougbo, N. S., Ikegwu, C. G., & Adewusi, A. O. (2024). Cybersecurity compliance in financial institutions: A comparative analysis of global standards and regulations. International Journal of Science and Research Archive, 12(01), 533-548.*
43. *World Bank, Digital Development Partnership, Cybersecurity Multi-donor Trust Fund & Tel Aviv University.(June 2023). Sectoral Cybersecurity Maturity Model. https://documents1.worldbank.org/curated/en/099062623085028392/pdf/P17263707c36b702309f7303dbb7266e1cf.pdf*
44. *World Economic Forum. (2021). Principles for Board Governance of Cyber Risk INSIGHT REPORT. https://www.weforum.org/publications/principles-for-board-governance-of-cyber-risk/*