Magna Scientia Advanced Research and Reviews

eISSN: 2582-9394

Cross Ref DOI: 10.30574/msarr

Journal homepage: https://magnascientiapub.com/journals/msarr/

(REVIEW ARTICLE)

Check for updates

Fragmentation and Harmonization of Cybersecurity and IT Control Frameworks: An Integrative Review of U.S. Governance Practices

William Asare Yirenkyi [1,*], Godson Teye Apaflo [2], Matilda Konotey [1] and Mary Magdalene Yeboah [3]

[1] *Temple University, Fox School of Business, Philadelphia, PA.*
[2] *Information Technology and Decision Sciences, University of Energy and Natural Resources.*
[3] *Department of Accounting, University of Ghana.*

Magna Scientia Advanced Research and Reviews, 2026, 17(02), 079–087

Publication history: Received on 30 May 2026; revised on 04 July 2026; accepted on 08 July 2026

Article DOI: https://doi.org/10.30574/msarr.2026.17.2.0127

Abstract

Cybersecurity and information technology control frameworks in the United States exhibit significant fragmentation arising from overlapping regulatory mandates and duplicated controls. Audits and compliance activities in financial institutions and critical infrastructure sectors identify vulnerabilities but reveal limitations when applied as static mechanisms rather than adaptive processes. Mapping exercises between National Institute of Standards and Technology Cybersecurity Framework, Control Objectives for Information and Related Technology, and International Organization for Standardization 27001 consistently document both shared requirements and gaps that widen with the introduction of artificial intelligence and machine learning. Federal harmonization efforts have produced initial coordination yet face persistent barriers from agency-specific mandates and scarce longitudinal outcome data. Governance practices navigate these tensions through sector-specific applications that balance operational demands against systemic interoperability needs. The empirical studies highlight the need for continued attention to framework alignment, regulatory coordination, and empirical validation if resilience is to match evolving threats. Effective integration of controls requires addressing both practical implementation challenges and broader policy structures that shape cybersecurity governance across regulated industries. These dynamics underscore the importance of reducing unnecessary duplication while preserving essential specialization to support more resilient national cybersecurity posture. Ultimately, achieving meaningful harmonization will depend on sustained policy coordination and the development of robust evidence on post-alignment outcomes. This review synthesizes cross-sector evidence to identify structural, operational, and technological barriers to harmonization, while proposing an integrative governance perspective grounded in recent empirical and policy literature.

Keywords: Cybersecurity Governance; Regulatory Fragmentation; Framework Harmonization; IT; Control Frameworks; Cybersecurity Compliance

1. Introduction

Cybersecurity has become one of the defining challenges facing organizations and regulators across the United States. Digital systems now support nearly every aspect of economic activity, making the security of information assets essential to national resilience, market stability, and public confidence (U.S. Government Accountability Office, 2024). Financial institutions, health-care providers, port authorities, and other critical infrastructure operators function in an environment where threats evolve rapidly, and the consequences of failure can extend far beyond any single organization. In response, governance practices have grown more elaborate. Policymakers and industry leaders rely on a collection of control frameworks and regulatory mandates designed to strengthen defenses. However, the very proliferation of these instruments has generated its own difficulties. Standards such as the National Institute of

* Corresponding author: William Asare Yirenkyi

Standards and Technology Cybersecurity Framework, Control Objectives for Information and Related Technology, and International Organization for Standardization 27001 coexist alongside sector-specific rules including the Gramm-Leach-Bliley Act, Federal Financial Institutions Examination Council guidelines, the Health Insurance Portability and Accountability Act, and Securities and Exchange Commission requirements. The result is a governance landscape marked by duplication, inconsistencies, and challenges in achieving coherent and effective protection (Aspen Digital, 2024).

This fragmentation is more than an administrative inconvenience. It imposes tangible operational costs. Organizations frequently implement overlapping controls, maintain duplicate documentation, and reconcile conflicting expectations from multiple oversight bodies. Smaller entities bear a particularly heavy burden because they lack the resources to navigate the array of requirements efficiently (Mussmann et al., 2020). Larger institutions also report that the administrative load diverts attention and funding away from genuine threat mitigation toward compliance activities. The situation is compounded by rapid technological change. Artificial intelligence, machine learning, and large language models introduce new risks that many legacy frameworks were never designed to address. Bias in algorithmic decision-making, privacy concerns surrounding massive data sets, and model risk in banking applications stretch existing standards in ways that expose gaps rather than fill them (Agbadamasi et al., 2025b). As innovation accelerates, the distance between regulatory design and technological reality widens, leaving organizations to improvise supplementary safeguards while regulators struggle to keep pace.

Harmonization has therefore surfaced repeatedly in policy discussions. Greater interoperability among frameworks and regulations could reduce unnecessary duplication, lower compliance costs, and improve overall security outcomes (Aspen Digital, 2024). Early federal coordination efforts have produced modest progress, but agency-specific mandates and differing sectoral priorities continue to slow meaningful alignment (U.S. Government Accountability Office, 2025). The evidence reflects this ongoing tension. Some studies examine how audits and compliance activities function as practical tools that surface control weaknesses in financial and port environments (Tetteh-Kpakpah et al., 2025). Others map the overlaps and gaps between major frameworks, documenting both shared strengths and persistent shortcomings (Essien et al., 2022). Still others explore the readiness of existing standards for emerging technologies, highlighting areas where updates are urgently needed (Abugri et al., 2026). Incentive structures embedded in current frameworks also receive attention, with researchers noting that many designs encourage minimum compliance rather than proactive defense (Wang, 2020). Cross-sector comparisons reveal further variation, as governance approaches that work well in one industry prove less effective in another (Djebbar & Nordström, 2023).

These dynamics matter because cybersecurity governance sits at the intersection of regulation, technology, and organizational behavior. When frameworks overlap without clear coordination, resources are wasted and security is undermined. When harmonization lags behind innovation, new risks go unaddressed. When evidence on long-term outcomes remains scarce, policymakers and practitioners lack the data needed to judge which approaches deliver genuine improvements. The United States therefore confronts a governance challenge that is at once structural and urgent. Recent scholarship published since 2020 offers valuable insight into these issues through case studies from financial institutions and port operations, comparative analyses of major frameworks, policy evaluations of federal coordination, and examinations of artificial intelligence readiness. Taken together, these works illuminate the practical realities organizations confront and the systemic barriers that must be overcome if cybersecurity governance is to become more coherent and resilient.

2. Audit and Compliance Practices in U.S. Financial Institutions and Critical Infrastructure Sectors

Cybersecurity audits uncover control weaknesses in United States financial institutions while reinforcing baseline regulatory adherence. Case analyses of major incidents show that routine audits enable early risk identification and corrective actions that maintain investor confidence (Tetteh-Kpakpah et al., 2025; Onyekwuluje et al., 2025). Capital-market audits linked to Securities and Exchange Commission guidelines routinely surface vulnerabilities first exposed by ransomware attacks and large-scale data breaches (Onyekwuluje et al., 2025). Compliance with the Gramm-Leach-Bliley Act, Federal Financial Institutions Examination Council standards, and Payment Card Industry Data Security Standard sets minimum benchmarks that push organizations toward proactive risk management rather than simple checkbox exercises (Onyekwuluje et al., 2025). Port operations display parallel patterns where audits expose gaps in control implementation as digitization gathers pace (Akoto-Bamfo & Donkor, 2025).

Adaptive defense systems turn static audit results into genuinely responsive tools. Financial institutions that blend audits with artificial intelligence-driven monitoring achieve noticeably larger reductions in threat scale than those relying on periodic reviews alone (Tetteh-Kpakpah et al., 2025). Compliance activities therefore serve as practical instruments that highlight mismatches between regulatory demands and real-world control performance. Sector-

specific pressures add distinctive demands to audit procedures and set them apart from broader corporate settings (-Bamfo & Donkor, 2025). These same practices strengthen stakeholder trust by demonstrating visible commitment to risk mitigation. Financial-sector participants increasingly treat well-executed audits as strategic assets that bring operational resilience into line with investor expectations. Critical infrastructure operators face comparable pressures but must adapt audit processes to unique operational realities. Empirical studies consistently acknowledge that these mechanisms deliver immediate diagnostic insight while underlining the shortcomings of purely static approaches. Audits and compliance therefore remain foundational components that organizations rely on to uphold regulatory standing and confront immediate cyber threats in demanding environments.

Such audit work reaches beyond routine verification when it incorporates real-time operational data into broader risk assessments. In financial institutions repeated case reviews show that audits often surface gaps in access control and incident response that conventional checklists miss (Sulistyowati et al., 2020). The diagnostic power of these reviews becomes especially useful when threats evolve quickly. Port operations gain similar advantages when audits take account of sector-specific realities where digitization opens new vulnerabilities along supply chains and physical-digital boundaries (Mussmann et al., 2020). Adding adaptive defense tools strengthens the entire process by letting organizations react immediately to findings instead of waiting for the next scheduled review cycle. Compliance with established information technology standards can therefore spark deeper cultural shifts toward proactive risk management (Roy, 2020).

When audits document concrete corrective actions after serious incidents, stakeholder confidence rises measurably. This shift intensifies pressure for stronger audit programs (Onyekwuluje et al., 2025). In capital-market settings the connection ties directly to regulatory obligations that require transparent reporting of control effectiveness. Port authorities face parallel expectations because audit results affect operational continuity and regulatory approvals. Consequently, audits and compliance extend their influence into strategic governance. Organizations use the resulting insights not only to meet external rules but also to guide internal decisions about resource allocation and technology investment. Distinct sector pressures further shape audit design with financial institutions focusing on data privacy and transaction integrity while critical infrastructure emphasizes physical-cyber convergence risks. These contrasts underscore the value of audit approaches tailored to specific operational contexts. The evidence shows that audits and compliance consistently furnish diagnostic benefits across regulated sectors while exposing the limits of static methods (Djebbar & Nordström., 2023).

A closer look at audit practices reveals their capacity to nurture organizational cultures that value continuous improvement rather than one-off compliance exercises. In financial environments, ongoing engagement with regulatory data and incident examples illustrates how audits feed into proactive risk management frameworks that reach beyond minimum standards. Port settings likewise demonstrate that audits uncover control gaps tied to digitization trends and prompt targeted operational enhancements (Akoto-Bamfo & Donkor, 2025). When organizations treat compliance findings as strategic assets they align cybersecurity efforts more closely with wider business goals. This alignment improves governance maturity and sharpens resource allocation choices. The diagnostic contribution of audits therefore operates on several levels at once. Sector-specific adaptations keep the process relevant to the distinct challenges facing financial institutions and critical infrastructure operators. Taken together these mechanisms help build more resilient operational environments throughout regulated United States sectors (Moeti et al., 2025).

3. Regulatory Fragmentation in Cybersecurity Governance

Federal cybersecurity rules continue to produce persistent fragmentation because different agencies issue overlapping mandates. Industry stakeholders repeatedly describe the resulting duplication as a heavy compliance burden that fails to deliver proportional gains in security outcomes (U.S. Government Accountability Office, 2024). Sector-specific regulations interact with broader frameworks and generate inconsistent requirements across financial services, healthcare, and critical infrastructure (Aspen Digital, 2024). Governance practices must therefore operate inside a landscape where identical core controls appear under several regulatory umbrellas at once.

Fragmentation becomes most visible when organizations try to satisfy simultaneous obligations under the National Institute of Standards and Technology Cybersecurity Framework, Securities and Exchange Commission rules, and sector-specific regulators. The administrative workload that follows pulls resources away from genuine threat mitigation and toward documentation and reporting (U.S. Government Accountability Office, 2026). Policy analyses note that early coordination attempts have offered only modest relief while agency-specific mandates stay firmly in place (U.S. Government Accountability Office, 2025). Regulatory environments in the United States thus maintain structural fragmentation that touches both large institutions and smaller entities struggling to stay compliant. This fragmentation also shapes how organizations allocate resources often leading them to emphasize certain compliance

areas at the expense of others. Stakeholders regularly point out that overlapping rules create inefficiencies that slow timely security improvements. The overall result appears in elevated operational costs and delayed incident response. These conditions illustrate the practical difficulties that emerge whenever multiple oversight layers function without adequate alignment. Governance practices must therefore keep balancing competing demands to preserve effective risk management throughout regulated sectors.

The overlapping character of federal rules leaves organizations facing redundant reporting obligations that consume substantial administrative effort. In financial services for instance multiple agency requirements produce duplicated work in risk assessment and control documentation (Sulistyowati et al., 2020). Healthcare and critical infrastructure sectors encounter parallel patterns when sector-specific mandates overlap with national frameworks. This structural fragmentation suggests that governance practices require constant negotiation of competing expectations that seldom mesh cleanly. The administrative load associated with these overlaps shifts attention from core threat mitigation to compliance paperwork. Policy perspectives observe that although initial coordination steps have occurred entrenched agency-specific approaches still restrict broader relief. Smaller entities in particular struggle with these fragmented demands and often incur higher relative compliance costs (Mussmann et al., 2020). The regulatory landscape therefore sustains conditions that test efficient governance across organization sizes.

Stakeholder accounts repeatedly link regulatory fragmentation to operational inefficiencies that lengthen incident response times. Organizations explain that satisfying multiple overlapping mandates forces them to favor documentation over proactive security work. The pattern appears consistently across financial services, healthcare, and critical infrastructure where the same core controls receive attention under differing regulatory lenses. The resulting inconsistencies point to fragmentation as a built-in feature of United States cybersecurity governance that influences both strategic planning and daily operations. Early coordination efforts have delivered some progress, but persistent mandates indicate that complete alignment remains distant. Governance practices therefore adapt to a regulatory setting marked by duplication and varying degrees of specificity. These realities underline the importance of balanced approaches that reduce fragmentation without sacrificing sector-specific protections (Djebbar & Nordström., 2023). The cumulative burden on smaller entities further demonstrates the wide scope of the challenge. Empirical studies show that regulatory fragmentation places measurable burdens on organizations that seek both compliance and effective threat mitigation. Policy analyses connect these burdens to diverted resources and slower security gains across regulated sectors. Sector-specific rules interacting with broader frameworks create a governance environment in which duplication is commonplace. This pattern indicates that structural fragmentation remains a central trait of United States cybersecurity oversight. Organizations respond by prioritizing selected compliance areas, yet the net effect restricts operational efficiency. Ongoing coordination may bring incremental relief, but entrenched mandates suggest fragmentation will continue as a lasting governance reality. The practical difficulties created by multiple oversight layers therefore call for sustained attention if more streamlined regulatory environments are to emerge (Moeti et al., 2025).

4. Overlaps and Duplication in IT Control Frameworks

National Institute of Standards and Technology Cybersecurity Framework, Control Objectives for Information and Related Technology, and International Organization for Standardization 27001 share extensive control requirements while preserving distinct emphases that generate duplication when organizations apply them together. Mapping exercises regularly locate overlapping domains in risk assessment, access control, and incident response (Essien et al., 2022). Organizations frequently put identical measures in place to satisfy several frameworks at once. Comparative studies of industrial standards document additional gaps that stem directly from the sheer number of standards rather than from any lack of coverage (Djebbar & Nordström., 2023).

Alignment optimization demonstrates that explicit crosswalks between International Organization for Standardization, National Institute of Standards and Technology, and Control Objectives for Information and Related Technology can cut redundancy without sacrificing comprehensiveness (Essien et al., 2022). Governance models nevertheless keep duplication because the frameworks developed independently over time. Selection decisions between National Institute of Standards and Technology and International Organization for Standardization 27001 rest on considerations of cost, certification processes, and organizational context rather than on clear superiority in security outcomes (Alshar'e, 2023). Information technology control frameworks in United States practice therefore display structural overlaps that complicate governance rather than simplify it. These overlaps reach into documentation requirements that organizations must fulfill under separate but closely related standards. The resulting administrative burden commonly produces inefficiencies in control implementation and monitoring. Comparative evaluations illustrate how such duplication affects overall governance maturity. Organizations seeking to optimize resources turn into mapping techniques that help minimize unnecessary repetition. The evidence observes that although the frameworks supply complementary strengths their simultaneous use demands careful coordination to prevent wasteful overlaps.

Governance practices gain when coordination succeeds yet they continue to wrestle with difficulties rooted in the separate evolutionary paths of each standard.

Shared control requirements across these frameworks mean organizations often repeat similar measures to achieve compliance. Duplication surfaces in risk assessment and incident response where the same activities receive attention under different standards (Sulistyowati et al., 2020). Mapping exercises indicate that explicit alignment can lower redundancy while retaining each framework's unique contributions. Governance models, however, preserve the overlaps because the standards were created at different times to meet different organizational needs. Selection processes between frameworks reflect practical factors such as cost and certification that shape adoption choices (Mussmann et al., 2020). Structural overlaps therefore create governance challenges that call for active management to avoid inefficiencies. Organizations gain from coordination strategies that limit repetition, but the independent histories of the frameworks keep duplication alive as a lasting feature. This situation affects maturity levels and resource optimization throughout United States practice.

Comparative evaluations link framework overlaps to administrative burdens that affect control implementation efficiency. Organizations regularly encounter documentation requirements that repeat across standards. The literature suggests that mapping techniques hold promise for relief, but the broader governance landscape still reflects challenges born of framework proliferation. Independent development of standards contributes to this state of affairs where complementary strengths coexist with structural duplication. Governance practices therefore require deliberate coordination to reach streamlined results (Djebbar & Nordström., 2023). The resulting inefficiencies show that overlaps complicate rather than support effective control of environments. Organizations continue to manage these conditions through optimization efforts that attempt to balance comprehensiveness with practicality. The separate evolution of frameworks sustains these difficulties as a defining element of information technology control governance (Moeti et al., 2025). These findings indicate that duplication is not solely a design flaw but a consequence of historically independent framework evolution, suggesting that full harmonization may be constrained by institutional path dependency

5. Emerging Technologies and Framework Readiness Gaps

Artificial intelligence and machine learning bring risks that legacy frameworks address only in part. Bias, privacy, and transparency difficulties in artificial intelligence-driven credit scoring and business intelligence surpass the reach of traditional controls (Agbadamasi et al., 2025a; Agbadamasi et al., 2025b). Model risk management in banking calls for validation frameworks that go beyond conventional cybersecurity standards (Abugri et al., 2026). Large language model commercialization reveals additional readiness gaps across Control Objectives for Information and Related Technology, International Organization for Standardization 42001, and National Institute of Standards and Technology Cybersecurity Framework (McIntosh et al., 2024).

Legacy frameworks built for stable conditions struggle to keep up with rapid technological change. Comparative gap analyses indicate that International Organization for Standardization 42001 supplies stronger opportunities for artificial intelligence governance, though it still needs updates to cover emerging risks (McIntosh et al., 2024). Regulatory frameworks such as the Federal Trade Commission Act and Health Insurance Portability and Accountability Act offer foundational oversight but prove inadequate for the scale and complexity of modern artificial intelligence applications (Agbadamasi et al., 2025b). Governance practices therefore encounter readiness gaps that widen as technology outpaced control frameworks. These gaps surface in areas such as algorithmic accountability and data protection that traditional standards do not fully cover. Organizations adopting the new technologies must therefore add supplementary safeguards. The evidence stresses that without targeted updates governance effectiveness declines in technology-intensive settings. Readiness assessments consistently find that current controls provide only partial coverage. The situation generates steady pressure for framework evolution to match the speed of innovation. Governance practices in regulated sectors must therefore incorporate emerging risk considerations to maintain adequate protection levels.

The arrival of artificial intelligence and machine learning produces risk profiles that legacy frameworks handle incompletely. Bias and privacy concerns in credit scoring and business intelligence point to limitations in traditional control designs (Agbadamasi et al., 2025a). Model validation requirements in banking suggest that conventional standards need extension to handle new risk categories (Abugri et al., 2026). Large language model applications expose further gaps that cut across multiple frameworks. Comparative analyses connect these gaps to the swift pace of technological advance that leaves framework updates behind. Governance practices face mounting pressure to supplement existing controls with targeted measures that address algorithmic and data protection issues. The evidence notes that partial coverage remains without deliberate evolution of standards (Mussmann et al., 2020). Organizations therefore meet situations in which innovation introduces risks that current governance structures manage only

inadequately. This dynamic emphasizes the necessity of framework adaptation if effectiveness is to endure in technology-driven environments.

Readiness gaps become most evident when organizations commercialize advanced technologies inside existing control structures. Comparative evaluations suggest that some frameworks provide better starting points for artificial intelligence governance, yet updates continue to be required. Regulatory foundations supply oversight but fall short when applied to complex modern applications (Sulistyowati et al., 2020). Governance practices therefore need to integrate new risk considerations to close these gaps. Empirical studies associate the challenges with reduced effectiveness in technology-intensive settings. Organizations must introduce supplementary safeguards to preserve protection levels. The continuing pressure for framework evolution signals that readiness shortfalls constitute a persistent governance reality. Regulated sectors keep confronting widening gaps as innovation accelerates. Effective practices therefore depend on proactive integration of emerging risk factors into control environments (Djebbar & Nordström., 2023).

6. Harmonization Efforts and Persistent Challenges

Harmonization principles put forward interoperability as one way to lessen regulatory inconsistencies across sectors. Policy documents call for coordinated approaches that keep sector-specific needs intact while cutting duplication (Aspen Digital, 2024). Federal initiatives have begun coordination, but considerable work lies ahead before meaningful relief appears (U.S. Government Accountability Office, 2024). Standards and practices in cybersecurity governance still display fragmentation in actual adoption even though mapping tools are available (Moeti et al., 2025).

Incentive structures inside existing frameworks often fail to encourage proactive defense beyond minimum compliance (Wang, 2020). The absence of longitudinal outcome data represents a critical limitation, as it prevents validation of whether harmonization efforts produce measurable improvements in cybersecurity performance. This evidence gap weakens both policy confidence and organizational willingness to invest in alignment initiatives (Sulistyowati et al., 2020). Cross-sector testing of audit and adaptive strategies concentrates mainly in finance and ports leaving wider applicability largely unexamined (Djebbar & Nordström., 2023). Harmonization therefore moves forward slowly amid enduring evidence deficits and structural barriers. These barriers include differing agency priorities that delay consensus on unified approaches. Organizations keep experiencing compliance burdens even as coordination discussions advance. The literature emphasizes that successful harmonization depends on both policy-level adjustments and practical implementation support. Evidence limitations further weaken confidence in current proposals. Governance practices must therefore confront these persistent challenges if sustainable alignment across frameworks and regulations is to be achieved. Continued work in this direction could eventually produce more streamlined oversight while safeguarding necessary specialization.

Harmonization principles suggest the possibility of fewer inconsistencies through interoperability steps that honor sector requirements. Policy views advocate coordinated strategies that reduce duplication without erasing specialization. Federal coordination has recorded early advances, though substantial effort remains before relief spreads widely. Governance standards continue to show fragmentation in real-world use despite the existence of mapping resources. Incentive structures imply that present frameworks reward minimum compliance more than proactive measures (Wang, 2020). The shortage of longitudinal outcome data limits assessment of harmonization benefits. Cross-sector testing stays focused on particular areas which narrows broader understanding. These circumstances indicate that harmonization advances gradually amid evidence shortfalls and structural obstacles. Agency priorities slow the building of consensus. Organizations face ongoing burdens even while coordination proceeds. Effective harmonization relies on combined policy and implementation support. Evidence constrains lower confidence in proposed solutions. Governance practices therefore need sustained attention to surmount persistent challenges (Moeti et al., 2025).

7. Incentive Structures and Behavioral Responses in Cybersecurity Governance

Incentive structures inside existing frameworks shape organizational behavior in cybersecurity defense. Policy perspectives observe that current designs tend to reward minimum compliance more than proactive risk reduction (Wang, 2020). Organizations respond by directing resources toward visible regulatory checkboxes rather than comprehensive threat mitigation. This pattern appears consistently in financial institutions and critical infrastructure sectors. Governance practices therefore mirror responses molded by the motivational features built into standards and regulations. The evidence suggests that incentive gaps restrict how far organizations go in pursuit of genuine resilience improvements. Behavioral responses differ according to organization size and sector context with smaller entities

encountering particular difficulties in balancing compliance costs against security investments. These dynamics show that framework design occupies a central place in determining governance outcomes (Alshar'e, 2023).

Stakeholder analyses connect incentive structures to compliance-oriented behaviors that limit wider defense enhancements. Organizations navigate these structures by devoting resources to meet immediately observable regulatory demands while setting aside less visibly rewarded activities (Sulistyowati et al., 2020). The resulting behavioral patterns indicate that governance effectiveness hinges not only on technical controls but also on motivational alignment. Financial institutions and port operations demonstrate how incentives affect audit and compliance practices. The evidence points out that stronger incentive mechanisms could stimulate more proactive approaches throughout regulated sectors. Governance practices keep adjusting to these behavioral realities as organizations look for optimal responses inside current frameworks. Persistent incentive gaps therefore stand as a structural factor that influences overall cybersecurity posture (Mussmann et al., 2020).

8. Cross-Sector Variations in Framework Application and Evidence Limitations

Cross-sector variations surface in the ways organizations apply cybersecurity frameworks and controls. Financial institutions and critical infrastructure entities display distinct patterns in audit and compliance implementation that mirror sector-specific operational demands (Tetteh-Kpakpah et al., 2025). Healthcare and capital market contexts add further contrasts in how regulatory requirements translate into governance practices. These variations suggest that framework application is not uniform across United States regulated sectors. Evidence limitations intensify the differences because longitudinal data on outcomes remain scarce (Mussmann et al., 2020). Governance practices therefore manage both sector-specific realities and wider evidence gaps that restrict comparative understanding. Empirical studies propose that expanded cross-sector testing could improve insight into framework effectiveness. Variations in application highlight the practical difficulties of reaching consistent governance outcomes (Djebbar & Nordström., 2023).

9. Future Research Directions

Future investigations should prioritize longitudinal studies that measure security outcomes following framework alignment and regulatory harmonization initiatives. Current evidence lacks robust post-implementation metrics that would demonstrate whether reduced duplication translates into measurable risk reduction. Research could examine cost-effectiveness across firm sizes to clarify incentive structures for smaller entities adopting harmonized controls. Comparative testing of audit and adaptive strategies beyond finance and ports would strengthen generalizability of findings to additional critical infrastructure sectors.

Cross-sector analyses of artificial intelligence governance readiness could illuminate how bias, privacy, and model risk challenges interact with legacy frameworks in diverse regulatory contexts. Empirical validation of International Organization for Standardization 42001 and updated National Institute of Standards and Technology Cybersecurity Framework applications in real-world large language model deployments would address existing readiness gaps. International comparisons of harmonization approaches could identify transferable principles while acknowledging unique United States federal structures. Studies might also explore stakeholder perspectives on interoperability standards to refine policy recommendations for reducing fragmentation without compromising sector-specific protections.

Quantitative assessments of investor and market responses to improved cybersecurity disclosures would link governance practices more directly to economic outcomes. Mixed-methods research combining technical control evaluations with organizational adoption barriers could provide actionable insights for framework developers. Longitudinal tracking of compliance burdens before and after coordination efforts would offer concrete evidence on harmonization progress. Such research directions would strengthen the empirical foundation for cybersecurity governance and support more effective integration of controls in evolving regulatory landscapes. Continued focus on these areas would help close persistent evidence gaps and advance both theory and practice in United States cybersecurity governance.

10. Conclusion

Cybersecurity governance in the United States operates inside a complex setting shaped by overlapping regulations, duplicated control frameworks, and rapid technological change. Audits and compliance activities deliver practical value in financial institutions and critical infrastructure yet reveal inherent limitations when used as static mechanisms.

Regulatory fragmentation creates operational burdens while harmonization efforts manage only incremental progress. Framework mapping reveals both shared strengths and persistent gaps especially when artificial intelligence and machine learning come into play. Evidence on long-term outcomes after alignment remains limited, which constrains informed policy decisions. The literature as a whole shows that fragmentation and harmonization remain locked in dynamic tension. Effective governance therefore demands ongoing focus on practical control implementation as well as systemic regulatory coordination if resilience is to match evolving threats.

This tension runs through multiple layers of practice and policy. Audits offer immediate diagnostic benefits but fall short without continuous adaptation. Regulatory environments produce duplication that pulls resources away from core security work. Information technology control frameworks share substantial elements, while keeping structural overlaps rooted in independent development histories. Emerging technologies expose readiness gaps that legacy standards were never built to handle fully. Harmonization initiatives hold promise through interoperability principles, thoughpersistent agency-specific mandates and evidence deficits continue to restrict their reach. Organizations must therefore steer through these realities by balancing sector-specific needs against broader systemic alignment. The lack of robust longitudinal metrics makes it harder to judge which approaches produce the most meaningful risk reduction. Stakeholders across regulated sectors regularly meet administrative inefficiencies that could be eased by more coordinated oversight. At the same time the swift pace of technological innovation requires proactive framework evolution if governance is to stay relevant. Ultimately the way forward rests on sustained commitment to cutting unnecessary duplication while protecting essential specialization. Such work would improve operational resilience, reduce compliance costs, and strengthen national cybersecurity posture in an interconnected digital landscape. Future advancements will likely depend on the integration of adaptive, data-driven governance models capable of aligning real-time risk signals with evolving regulatory expectations, thereby bridging the gap between compliance structures and operational cybersecurity effectiveness.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Agbadamasi, T., Opoku, L. K., Adukpo, T. K., & Mensah, N. (2025a). Artificial intelligence governance in U.S. corporations: Legal and ethical implications for business intelligence and regulatory compliance. International Journal of Research Publication and Reviews, 6. 2582-7421. 10.55248/gengpi.6.0325.11124.

[2] Agbadamasi, T., Opoku, L. K., Adukpo, T. K., & Mensah, N. (2025b). Navigating the intersection of U.S. regulatory frameworks and artificial intelligence: Strategies for ethical compliance. World Journal of Advanced Research and Reviews, 25(3), 969–979.

[3] Akoto-Bamfo, D. & Donkor, A. A. (2025). A critical review of IT audit practices for compliance in port operations in the U.S. Sarcouncil Journal of Engineering and Computer Sciences, 4(12).

[4] Alshar'e, M. (2023). Cyber security framework selection: Comparison of NIST and ISO27001. Applied Computing Journal.

[5] Aspen Digital. (2024). A security symphony: Harmonizing cybersecurity regulation. Aspen Institute. https://www.aspendigital.org/report/security-symphony/

[6] Djebbar, F. & Nordström, K. (2023). A comparative analysis of industrial cybersecurity standards. IEEE Access PP (99):1-1.

[7] Essien, I. A., Cadet, E., Ajayi, J. O., Erigh, E. D., Obuse, E., Ayanbode, N., & Lawal, A. B. (2022). Optimizing cyber risk governance using global frameworks: ISO, NIST and COBIT alignment. Journal of Frontiers in Multidisciplinary Research 3(1):618-629.

[8] McIntosh, T. R., Susnjak, T., Liu, T., Watters, P., Xu, D., Liu, D., Nowrozy, R., & Halgamuge, M. N. (2024). From COBIT to ISO 42001: Evaluating cybersecurity frameworks for opportunities, risks, and regulatory compliance in commercializing large language models. Computers & Security, volume 144, 103964. https://doi.org/10.1016/j.cose.2024.103964

[9] Moeti, W., Moyo, S., & Kanzi, A. (2025). Compliance and Control: Standards and practices in cyber security governance. Research Square.

[10] Mussmann, A., Brunner, M., & Breu, R. (2020). Mapping the State of Security Standards Mappings. 10.30844/wi_2020_l4-mussmann.

[11] Abugri, C., Pallapati, J., & Nketiah, T. A. (2026). Model risk management and validation frameworks for machine learning models in banking: A comprehensive review.

[12] Onyekwuluje, T. P., Akoto-Bamfo, D., Tetteh-Kpakpah, C., Panful, B., & Oware, D. (2025). Evaluating the role of cybersecurity audits in protecting the US capital market. World Journal of Advanced Research and Reviews, 25(2), 974–980. https://doi.org/10.30574/wjarr.2025.25.2.0183

[13] Onyekwuluje, T. P., Tetteh-Kpakpa, C., Panful, B., Apaflo, B. N., & Donkor, A. A. (2025). The role of IT compliance in enhancing cybersecurity measures for U.S. financial institutions. International Journal of Research Publication and Reviews, 6(1), 2600–2606.

[14] Roy, P. P. (2020). High-level comparison of NIST Cyber Security Framework and the ISO 27001 Information Security Standard. 1-3. 10.1109/NCETSTEA48365.2020.9119914.

[15] Sulistyowati, R., Handayani, F., & Suryanto, Y. (2020). Comparative analysis and design of cybersecurity maturity assessment methodology using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS. JOIV International Journal on Informatics and Visualization 4(4):225-230.

[16] Tetteh-Kpakpah, C., Adjaottor, S., & Donkor, A. A. (2025). Mitigating cyber threats through cybersecurity audits and adaptive defense: A case study on financial institutions. EPRA International Journal of Economic and Business Review, 13(7).

[17] U.S. Government Accountability Office. (2024). Cybersecurity: Efforts initiated to harmonize regulations, but significant work remains (GAO-24-107602). https://www.gao.gov/products/gao-24-107602

[18] U.S. Government Accountability Office. (2025). Cybersecurity regulations: Industry perspectives on impact, progress, challenges, and opportunities of harmonization. (GAO-25-108436). https://www.gao.gov/products/gao-25-108436

[19] U.S. Government Accountability Office. (2026). Cybersecurity regulations: Additional industry perspectives on impact, progress, challenges, and opportunities of harmonization. (GAO-26-108685). https://www.gao.gov/products/gao-26-108685

[20] Wang, B. (2020). Rethinking existing cybersecurity frameworks: How to incentivize companies to better defend against cyber threats [Doctoral dissertation]. ProQuest.