The analysis of cybersecurity audit standards in different parts of the world in the context of digital transformation

Olesya Voytovych, Vitalii Volynets

Vinnytsia National Technical University, Vinnytsia, Ukraine

Abstract

This article compares cybersecurity obligations across the EU, North America, Asia, and Africa in four sectors (finance, healthcare, IT, retail). Drawing on a desk review of statutory and industry sources (e.g., GDPR/NIS2/DORA; GLBA/FTC Safeguards/HIPAA; MLPS 2.0/PIPL; POPIA; PCI DSS), it maps where control expectations converge risk analysis, access management, encryption, incident reporting and where they differ in enforceability and evidence requirements. We find that multinational programs often duplicate audits and still miss operational readiness in cloud and supply-chain scenarios. The study concludes by proposing the development of an integrated compliance model and a Unified Control Framework to address these issues.

Keywords

digital transformation; information security; cybersecurity; cybersecurity audit; global cybersecurity standards.

1. Introduction

Digital transformation has increased dependence on cloud and third-party services, exposing organizations to recurring risks such as ransomware, supplier compromise, and cloud misconfiguration. At the same time, companies operate under overlapping international, national, and industry frameworks with different expectations for controls and audit evidence.

We compare cybersecurity obligations across the EU, North America, Asia, and Africa in finance, healthcare, IT, and retail. Based on a desk review of statutes and major standards, we identify common control themes and meaningful divergences in enforceability and assurance. Our results indicate duplicated audits alongside gaps in testing real-world readiness, especially for cloud and supply chains. We propose a jurisdiction-aware control map that ties obligations to testable safeguards and supports a lean evidence pack.

2. Problem Statement

Multinational programs face overlapping cybersecurity obligations that lead to repeated audits, fragmented controls, and weak evidence of real-world readiness. What is missing is a compact, jurisdiction-aware mapping from obligations to normalized controls and to outcome-based tests with a minimal evidence pack. We propose and evaluate such a mapping with regional overlays and an adaptive audit approach aimed at cutting duplicate work while improving coverage of scenario-based testing.

3. Analysis of Recent Research and Publications

Recent work shows that digital services scale across borders while cybersecurity governance remains tied to jurisdictions and is growing more divergent. For multinational firms, this fragmentation produces overlapping and sometimes conflicting obligations shaped not only by risk considerations but also by geopolitics [1].

Studies describe the operational burden as “compliance” or “audit” fatigue: overlapping rules lead to repeated assessments, duplicated documentation, and the diversion of scarce security staff from preventive work to audit preparation. This dynamic encourages check-the-box behavior, where passing an assessment can outweigh improving control performance [2].

Evidence also indicates that documentation-led compliance does not reliably translate into resilience. Cloud and supply-chain exposures, in particular, remain under-tested when effort

concentrates on paperwork. The literature therefore calls for integrated, jurisdiction-aware control mappings and more outcome-based verification (e.g., scenario-driven tests) to close the gap between formal compliance and real protection [3].

4. Research Results

A cross-sector comparison across the EU, North America, Asia, and Africa shows recurring control priorities — structured risk management, identity and access governance, encryption, monitoring, and incident handling — yet materially different philosophies about enforceability, accountability, and audit evidence. These contrasts affect how programs are designed and how assurance is demonstrated in practice.

Regulation in financial services is uniformly strict, but the route to assurance diverges by region. The EU's DORA adopts a prescriptive stance: integrated ICT-risk governance, regular continuity exercises, and threat-led penetration testing (TLPT) for significant entities on a multi-year cadence — at least every three years [4, 5]. North America's GLBA takes an accountability-first approach. The Safeguards Rule assigns a Qualified Individual to run a risk-based program and calls out foundational safeguards such as encryption of customer information, multi-factor authentication, and activity logging [6]. China's MLPS 2.0 reflects a state-directed doctrine organized around the "one center, three layers of protection"; where "Important Data" are in scope, Level 3 obligations commonly entail stronger network zoning and separation of development from production environments [7]. Principle-based regimes in Africa, exemplified by South Africa's POPIA, require "appropriate, reasonable technical and organisational measures," which in practice drive encryption, RBAC, least-privilege access, and MFA for critical systems [8]. Given this spread, multinational firms gain more from a modular GRC architecture with regional overlays than from a single global policy.

Patient-safety considerations make the healthcare domain distinctive: confidentiality, integrity, and availability all carry direct consequences. Within the EU, GDPR together with NIS2 compels technical-organizational measures (e.g., pseudonymization, encryption) and mature processes for risk analysis, incident response, and supplier oversight [10]. HIPAA in North America is technology-neutral and distinguishes "required" from "addressable" safeguards, permitting justified substitutions — including for encryption-provided the rationale is documented. Several Asian jurisdictions classify healthcare as Critical Information Infrastructure, which triggers stricter governance requirements, dedicated security bodies, personnel vetting for sensitive roles, and annual risk assessments. African frameworks, with POPIA as a reference point, treat health data as "special personal information," rendering processing unlawful by default unless narrow conditions — explicit consent, legal necessity, or defined research purposes — are satisfied [11]. Across these settings, the difference is less about whether to implement encryption or access control and more about the evidence supervisors expect and the penalties for failure.

Rules that govern the IT supply side often double as instruments of industrial policy. The EU's NIS2 establishes baseline measures across essential and important entities and introduces personal accountability for governing bodies in cases of non-compliance [12]. Market assurance carries more weight in North America via SOC 2: organizations scope audits to the five Trust Services Criteria, with Security the only universal requirement, which allows flexible alignment with business models while still signaling assurance to customers [13]. China operationalizes MLPS 2.0 as a formal, state-supervised certification pathway that can function as a gate to market entry. In many African markets, ISO/IEC 27001 certification is a deliberate strategic signal of a formal ISMS while sector-specific regimes continue to mature, helping local providers win contracts with global partners.

E-commerce's expansion has reshaped the retail baseline, pairing scale with trust. The EU operationalizes GDPR through data-subject-rights processes-data minimization, consent management, and dependable handling of access and deletion requests alongside security of processing. North America's dominant scheme is PCI DSS, a contractual regime from the card brands; version 4.0 strengthens expectations around network security, cryptography, and multi-factor authentication for access to the cardholder data environment. China's PIPL adds consent and, for higher-risk processing, a Personal Information Protection Impact Assessment; it also restricts discriminatory pricing driven by automated decision-making. Across rapidly growing African markets, the policy goal is to build foundational consumer trust; Kenya's Data Protection Act

exemplifies this orientation by entrenching purpose limitation and data minimization as prerequisites for sustainable growth [14].

Table 1

Cybersecurity Standards for the Retail Sector (Summary)

Region	Key Laws and Standards	Key Incentives
EU	GDPR, NIS2, PCI DSS	GDPR Fines / PII Protection
North America	CCPA (California), PCI DSS, NIST CSF	PCI DSS / Litigation
Asia	China: PIPL, e-commerce laws	State Control / Data Localization
Africa	National data protection laws	Consumer Rights / Fraud Prevention

Across sectors and regions, shared ground is clear, but so are the splits: how mandatory measures are, what evidence supervisors expect, who is held to account, and whether data must remain domestically stored. Data-localization rules crystallize the divide. China requires domestic storage and transfer controls for personal and "important" data particularly for critical infrastructure whereas the EU permits cross-border transfers subject to adequate safeguards rather than a blanket storage mandate inside the Union.

For multinational programs, a single, static policy is unlikely to span these variations. A more workable path is a modular compliance and assurance stack: a core control set mapped to common obligations; regional overlays where law or supervisory practice demands more (e.g., TLPT cadence under DORA [4], [5] or level-based measures under MLPS 2.0 [7]); and a compact evidence pack that emphasizes outcome-oriented tests over paperwork. Such a design reduces duplicate audits, aligns documentation with real-world readiness in cloud and supply-chain scenarios, and leaves room for sector-specific enforcement models from EU legal mandates to North American market attestations and African capability-building anchored in ISO/IEC 27001 and emerging data-protection statutes.

5. Conclusions

Our analysis reveals that despite shared global trends, regional regulatory philosophies remain the primary force shaping corporate cybersecurity systems. The analysis demonstrated fundamentally different regulatory approaches: from the strictly regulated in the EU to the flexible in the US, state-controlled in Asia, and fragmented but developing in Africa. This highlights the insufficient unification of existing approaches and creates significant difficulties for international companies.

Based on these findings, we propose that future research should focus on developing an integrated compliance model that would allow for the dynamic adaptation of internal controls to the specific requirements of different jurisdictions, thereby minimizing the regulatory burden. Modern companies face exhaustion from a surplus of regulations, performing numerous, often redundant, audits. This creates an urgent need to harmonize audit practices through the creation of a Unified Control Framework that maps the requirements of key standards. Furthermore, it was found that formal compliance does not always guarantee actual cyber resilience. Consequently, a relevant task is to develop a flexible cybersecurity maturity assessment model that integrates technical and organizational aspects and allows for scenario-based testing to verify real-world preparedness for cyberattacks.

References

[1] A. Kuzior, I. Tiutiunyk, A. Zielińska, R. Kelemen, Cybersecurity and cybercrime: Current trends and threats, *Journal of International Studies* 17 (2024) 220–239. doi:10.14254/2071-8330.2024/17-2/12.

[2] O. Ilori, C. E. Lawal, S. C. Friday, J. Ibine, E. C. Eke, D. R. Tolulope, Cybersecurity auditing in the digital age: A review of methodologies and regulatory implications, *Journal of Frontiers in Multidisciplinary Research* 3 (2022) 174–187. doi:10.54099/IJFMR.2022.0301.174.

[3] A. Folorunso, I. Wada, B. Samuel, V. Mohammed, Security compliance and its implication for cybersecurity, *World Journal of Advanced Research and Reviews* 24 (2024) 2105–2121. doi:10.30574/wjarr.2024.24.1.3170.

[4] S. J. Ursillo Jr., K. Manske, B. Kirk, CMMC programmatic final rule status: What it means for defense contractors, 2025. URL: https://www.cbh.com/insights/articles/cmmc-compliance-and-its-implications-for-defense-contractors/.

[5] M. Osiashvili, The key role of the most recent EU regulation – the "Digital Operational Resilience Act" in the legal system, contemporary challenges, and Georgian perspectives, *European Scientific Journal (ESJ)* 20 (2024) 1–16. doi:10.19044/esj.2024.v20n26p1.

[6] M. Toussaint, S. Kirmé, H. Panetto, Industry 4.0 data security: A cybersecurity frameworks review, *Journal of Industrial Information Integration* 39 (2024) 100694. doi:10.1016/j.jii.2024.100694.

[7] R. Creemers, China's emerging data protection framework, *Journal of Cybersecurity* 8 (2022) tyac011. doi:10.1093/cybsec/tyac011.

[8] T. Chimboza, E. Smith, How does compliance with the Protection of Personal Information Act (POPI Act) affect organisations in South Africa?, in: *Proceedings of the 10th Annual African Conference on Information Systems and Technology (ACIST 2024)*, Kennesaw, GA, USA, 2024. URL: https://digitalcommons.kennesaw.edu/acist/2024/presentations/19.

[9] I. M. Dorosh, Cybersecurity and its role in the financial sector: Threats and protection measures, *Economics. Finances. Law* 10 (2023). doi:10.37634/efp.2023.10.10.

[10] M. van 't Schip, The regulation of supply chain cybersecurity in the NIS2 Directive in the context of the Internet of Things, 2024. doi:10.2139/ssrn.4848048.

[11] P. Ewoh, T. Vartiainen, Vulnerability to cyberattacks and sociotechnical solutions for health care systems: Systematic review, *JMIR Medical Internet Research* 26 (2024) e46904. doi:10.2196/46904.

[12] P. G. Chiara, Towards a right to cybersecurity in EU law? The challenges ahead, *Computer Law & Security Review* 53 (2024) 105961. doi:10.1016/j.clsr.2024.105961.

[13] O. Deineka, O. Harasymchuk, A. Partyka, A. Obshta, N. Korshun, Designing data classification and secure store policy according to SOC 2 Type II, in: *Cybersecurity Providing in Information and Telecommunication Systems 2024*, vol. 3654, 2024, pp. 398–409.

[14] B. Trivedi, Retail cybersecurity in the agentic age: Securing autonomous shopping agents in e-commerce, *European Modern Studies Journal* 9 (2025) 52. doi:10.59573/emsj.9(4).2025.52.