Sarcouncil Journal of Engineering and Computer Sciences

ISSN(Online): 2945-3585

Volume- 05| Issue- 03| 2026

Review Article

Received: 01-02-2026| Accepted: 25-02-2026 | Published: 12-03-2026

A Literature Review of Secure Digital Transformation Practices in Regulated Sectors

Karyn Ekpo

University of West Georgia – Richards College of Business, Georgia, USA

Abstract: Digital transformation (DT) in regulation-sensitive domains, such as finance, healthcare, energy, and public administration, is characterized by both innovation opportunities and increased cyber risk. Security enforcement in these situations must integrate governance policies, regulatory stipulations, technical defenses, and business processes. This paper provides a narrative and state-of-the-art review of what is known regarding safe DT practices in the US context and beyond, drawing on relevant literature, types of regulatory guidance, and practitioner frameworks. The latest research on digital transformations indicates that secure DT is becoming more rooted in governance structures like the U.S' National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0, the Secure Software Development Framework (SSDF), and the Cybersecurity and Infrastructure Security Agency (CISA) Zero Trust Maturity Model, which are increasingly promoting secure-by-design engineering together with resilience and accountability. Compliance models like Health Insurance Portability and Accountability Act (HIPAA), Federal Financial Institutions Examination Council (FFIEC) guidance, North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) enforcement and European Union (EU) tools such as Network and Information Security 2 **(**NIS2)/Digital Operational Resilience Act (DORA) and the Cyber Resilience Act implant enforceable obligations raising accountability in management. Through technology-empowered practices such as DevSecOps, Zero Trust architectures, cloud security baselines and supply chain assurance, these mandates are operationalized across several industries. This review synthesizes regulatory, technological, and human dimensions shaping secure DT. It also touches upon human and organizational aspects, with culture, knowledge level, insider threats, and management buy-in continuing to be crucial factors for success. Nevertheless, gaps with an array of core issues remain. Some identified are regulatory alignment, enforcement consistency, supply chain visibility, Artificial Intelligence (AI) governance and metrics for secure DT effectiveness. The paper argues that sustainable change can only be achieved through a mix of flexible technical mechanisms alongside prescriptive hard law, organizational cultural transformation, and resilience strategies. By highlighting what is currently being done and contributing to identifying where work needs to be done, this review offers a map for policy makers, regulators, and organizations who are charged with delivering secure digital transformation in regulated enterprises.

Keywords: Secure Digital Transformation, Regulated Sectors, Cybersecurity Governance, Compliance, Frameworks, Zero Trust Architecture, Resilience.

INTRODUCTION

DT in regulated sectors cannot be separated from cybersecurity governance. Financial services, healthcare, energy/utilities, and, to a lesser extent, public administration are digitizing business-critical processes under the burden of heavy regulatory requirements and hostile threat activity. U.S. policy has shifted decisively towards Zero Trust and secure-by-design practices, via the federal mandate that is forcing agencies to adopt pervasive strong identity, device posture, encrypted traffic, and internet-accessible application patterns on path with a zero-trust architecture (ZTA) baseline (Young 2022). Concurrently, the CISA Zero Trust Maturity Model (ZTMM) v2.0 translates this model into practical pillars (identity, devices, networks, applications/workloads, data) and cross-cutting capabilities, providing a maturity trajectory that non-federal organizations can leverage to organize transformation spending and measures (CISA, 2023).

On the software and supply chain level, the modern digital transformation substrate, NIST's Secure Software Development Framework (SSDF), provides a common, auditable language of practices for producers and acquirers. SSDF v1.1 puts in place Software Development Life Cycle (SDLC) practices to protect against vulnerabilities and attends to purchasing needs of buyers, to stand as a dock for regulated buyers who must ask vendors for evidence (Souppaya *et al.,* 2022). The CISA 2023 summary highlights that organizations must implement SSDF within the company and express supplier requirements using the SSDF convention, which bridges governance and acquisition (Souppaya *et al.,* 2022). As a state-of-the-art example, it can be argued that NIST's Special Publication 800-218A scales SSDF to generative AI and dual-use base model challenges with secure-by-design responsibilities over the model lifecycle development and integration processes in a manner each prescriptive for regulated entities

***Corresponding Author:** Karyn Ekpo

DOI- https://doi.org/10.5281/zenodo.18988452

commandeering adoption of AI technologies for clinical operations, financial applications/categorization decisions (Booth *et al.,* 2024).

The regulatory environments are converging toward both resilience and accountability. In the EU, NIS2 extends the sectoral scope of regulation (almost reaching digital economy), codifies risk management measures, and raises top-management responsibilities and reporting standards, with ensuing reverberations for global supply chains and multinationals (European Commission, 2024). In financial services, the Digital Operational Resilience Act (DORA) introduces standardized requirements for Information and Communication Technology (ICT) risk governance, incident reporting testing, and third-party controls. The regulation's official text stipulates the binding mechanisms and their scope for firms to operationalize across digital transformation programs (Regulation, 2022). Sectoral supervisors such as European Insurance and Occupational Pensions Authority (EIOPA) have made available compact overviews that link the legal mandates of DORA to supervisory practice (EIOPA, 2025).

In the U.S., operational transformations within the energy industry are beginning to bring systemic risk concerns and attention from both standards and regulatory perspectives. Primer-style guides that interpret NERC CIP provide readers with a quick map of duties around bulk electric system cybersecurity (for example, supply-chain and network monitoring) that organizations must factor into modernization road maps (NERC CIP Standard, 2024). On a practical level, new or moving policy steps, such as Federal Energy Regulatory Commission (FERC) actions on Bulk Electric System (BES) cybersecurity, indicate how resilience expectations continue to expand with increased digitization (Nicholas, 2025).

Healthcare demonstrates exactly why secure digital transformation must address policy, technology, and human factors. Media reports about proposed U.S. regulations to enhance protections for healthcare data underscore the policy drumbeat that has emerged in response to ongoing harms from breaches and operational disruptions (Wes Davis, 2024). Within the organizations, information-security management requires a comprehensive, audited system that includes confidentiality, integrity and availability alongside staff training, governance and room for improvement (Nowicka *et al.,* 2024). These foundational management practices supplement sector-specific security regimes and technical architecture.

Supply-chain assurance is the connective tissue of secure digital transformation across industries. NIST Special Publication 800 Series contains multi-level guidance (enterprise, mission/business, operational) to address the cybersecurity risk within supply chain, which includes control families, measurement topics, and templates that program management can adopt (Boyens *et al.,* 2022). In combination with SSDF (and, where appropriate, AI-specific profiles), these artifacts support how regulated organizations can translate policy goals into actionable engineering and procurement practices (Souppaya *et al.,* 2022; Booth *et al.*, 2024).

Lastly, the governance environment continues to evolve. NIST Cybersecurity Framework (CSF) 2.0 press release shows the focus on the new "Govern" category and measurable outcome to provide boards and C-level executives with a language guiding secure digital transformation that can be held accountable (Boutin, 2024). In the context of the public sector, the U.S. Office of Management and Budget's (OMB) zero trust strategy weaves policy into practice through tangible identity, encryption, and app-exposure demands, a move that is increasingly representing patterns for emulation and adaptation by state/local entities as well as regulated private enterprises (Young, 2022; CISA, 2023).

This state-of-the-art review is a narrative synthesis of U.S. and global practice on five themes: governance, compliance, technology enablement, human factors and resilience, with selective citation from academic literature, government publications, and press releases to ground claims in authorities' frameworks, legal codes, or sector exemplars. It contextualizes how secure-by-design engineering (SSDF, AI profiles), zero-trust architecture (OMB/CISA) and supply-chain assurance operationalizes regulatory goals (NIS2, DORA, GDPR Art. 32) among sector-specific pressures (energy, healthcare and finance), and aims at exposing theoretical and policy gaps by highlighting what is currently being done and contributing to identifying where work needs to be done (European Commission, 2024; Regulation, 2022; GDPR, 2025) among sector-specific pressures (energy, healthcare and finance), and aims at exposing theoretical and policy gaps by highlighting what is currently being done and

Publisher: SARC Publisher

contributing to identifying where work needs to be done, this review offers a map for policy makers, regulators and organizations who are charged with delivering secure digital transformation in regulated enterprises (European Commission, 2024; Regulation, 2022; GDPR, 2025).

Governance Frameworks in Secure Digital Transformation

Good governance structures are fundamental in ensuring that digital transformation is rolled out securely and sustainably across heavily regulated industries. By governance, we mean the practice of harmonizing policies, organization structures, risk management practices, and compliance activities with emerging cyber risks and regulatory requirements. In the U.S. and across E.U., the NIST Cybersecurity Framework (CSF 2.0), Secure Software Development Framework (SSDF), Zero Trust models, as well as sector-specific rules such as FFIEC, NERC CIP, DORA, NIS2, influence how organizations enact and measure secure transformation efforts.

U.S. Federal Governance Anchors

The U.S. approach is primarily driven by policy. OMB Memorandum M-22-09 details a federal Zero Trust approach that mandates agencies to have identity, device, network, application, and data protection in place by Fiscal Year 2024 (FY2024). This binding governance document compels agencies to show measurable progress across Zero Trust (ZT) pillars and begins to set a model that state and local governments and regulated private companies are finally following. In addition to this, there is new version developed, which is CISA Zero Trust Maturity Model v2. 0. The federal government operationalizes this strategy with incremental levels of maturity for each pillar (Identity, Devices, Networks, Applications/Workloads, Data) and a framework for cross-cutting governance, visibility, and automation (CISA, 2023).

Governance spans software assurance as well. NIST SP 800-218 (SSDF v1.1) represents a "set of high-level secure software development practices that can be incorporated into all SDLCs" (Souppaya *et al.,* 2022). It focuses on governance outcomes, specifying security demands, securing development environments, and responding to vulnerabilities rather than tools; so, the practices are generic and can be applied across the board. Its 2024 companion, NIST SP 800-218A, refines these recommendations for generative AI and dual-use foundation models with a caution that "AI model producers need to be safeguarding their model weights, pipelines, reward models to the same standards as traditional code" (Booth *et al.,* 2024). This thereby situates governance not just as control but as adaptive regulation in emerging AI-enabled DT.

Another governance focus is supply-chain assurance, for instance, procurement under Executive Order 14028. Cybersecurity Supply Chain Risk Management (C-SCRM) is an increasingly important practice area defined by NIST SP 800 as a "systematic process for managing the cyber supply chain risk to ensure that the risk is at an acceptable level" (Boyens et al, 2022). This injects governance on three levels (enterprise, mission/business, operational) and requires corporate-level ownership and policy templates, along with cross-functional program management. Incorporating C-SCRM into risk framing, assessment, response and monitoring, this guidance establishes board-level responsibility for procurement and vendor management.

U.S. Sectoral Governance Models

Sector regulators broaden federal rules to sectoral requirements. Within financial services, the FFIEC Information Technology (IT) Handbook dictates governance of an information security program, which includes oversight by the board, risk assessments, and third-party management. FFIEC Architecture, Infrastructure, and Operations (AIO) booklet takes it one step beyond, addressing governance against resilience objectives, cloud adoption, and Zero Trust adoption. In energy, the NERC CIP standards formalize governance of operational technology, requiring documented policies for incident reporting, configuration, and supply chain risk reduction. The FERC's July 2025 order goes a step further in establishing governance standards by placing an obligation on utilities to implement controls to ensure that they have minimized the cyber risk, potentially creating a floor for regulatory expectations regarding cybersecurity assets ranging across the bulk electric systems, sending regulators' intentions toward cyber risks. In healthcare, governance is changing under U.S. Department of Health and Human Services (HHS) proposals that more tightly regulate health data to reflect ongoing breach patterns.

European Union Governance Models

The EU governance framework ensures management in law. NIS2 Directive (European Commission, 2024) requires that the management

Publisher: SARC Publisher

bodies of these entities receive, validate and approve their cybersecurity risk measures, or be potentially liable for a failure (CISA, 2023). Meanwhile, the Digital Operations Resilience Act (DORA) also requires financial institution boards to endorse ICT risk strategies, impose internal governance frameworks and supervise third parties that supply their ICT support. It enshrines this in law (Regulation (EU) 2022/2554), taking business governance from being merely good practice into a legal obligation. This is a model of governance where cyber risk becomes the business of the board and can be enforced by the likes of EIOPA.

Comparative and Integrative Governance Developments

Comparing the U.S. and E.U. approaches highlights both points of convergence and divergence. Technical frameworks (SSDF, Zero Trust) are operationalized through executive orders and federal memos in the U.S. Under EU governance, accountability is encoded in law, and board members are directly responsible for failures to oversee cyber risk. Both models end up as governance equals accountability plus assurance, involving documentation, measurement, and reporting. Sectoral frameworks such as FFIEC, NERC CIP, and healthcare rules tie governance to resiliency; EU frameworks like NIS2 and DORA link it to compliance and liability.

Governance Challenges and Gaps

Despite progress, gaps remain. Former governance models favoring "blind trust" remain in place and are in opposition to Zero Trust frameworks, keeping transformation at bay. The governance of supply chains is fragmented; while NIST 800-161 is explicit with its guidance, there is no common enforcement across agencies or sectors. Enforcement capacity for NIS2 and DORA within the EU is hugely variable, which raises harmonization issues. Lastly, in the U.S. and EU alike, governance of AI adoption in regulated sectors is underdeveloped, while NIST 800- 218A consists of technical guidance, not legal and organizational accountability frameworks for AI security.

The assessed governance frameworks have high levels of coordination between strategic management and technical implementation. One of the key advantages of the U.S. approach is that NIST and CISA models are flexible and enable organizations to make governance structures context-specific. Their status is, however, mainly voluntary, and thus restricts uniform enforcement, unlike EU frameworks such as NIS2 and DORA, which are binding in terms of accountability but may have little flexibility to reflect the differences in the sector.

Compliance and Regulatory Landscape

Compliance Frameworks are the key to secure digital transformation in regulated industries. Compliance, unlike governance, which focuses on structures and oversight, codifies enforceable obligations, reporting responsibilities, and penalties. This section synthesizes the primary compliance regimes in the US and EU, as well as internationally, revealing how they influence sectoral change while also standing out as enduring challenges.

Financial Services

The financial services are among the most tightly regulated industries due to their systemic functions. In the U.S., the Information Security Booklet (2016) of the FFIEC IT Handbook requires institutions to develop an enterprise-wide information security program that specifies safeguards to maintain the confidentiality, integrity and availability of sensitive customer information. The manual emphasizes board-approved policies, risk assessments and ongoing program updates reflecting advances in technology and changing threats. Its Architecture, Infrastructure and Operations (AIO) Booklet (2021) broadens that compliance expectation to include cloud adoption, Zero Trust and resilience testing.

At the international level, Basel Committee's Principles for Operational Resilience (2021) imposes banks to formalize cyber resilience into compliance obligations with focus on governance, ICT dependencies and third-party risk structures (Supervision, 2021). These principles are consistent with U.S. rules by incorporating resilience as part of prudential supervision. In Europe, the Digital Operational Resilience Act (DORA) establishes a common standard for ICT risk management, an obligation to report incidents and manage critical third-party providers at EU level in finance (European Commission, 2024). The regulation (EU 2022/2554) came into effect with January 2025 compliance obligations, which made resilience a matter of law. Supervisors like EIOPA issue interpretative guidance, casting in practice these requirements across jurisdictions.

Healthcare

Healthcare compliance structure balances the patients' security with their privacy. In the United

Publisher: SARC Publisher

States, legislation like the HIPAA Security Rule imposes requirements for electronic protected health information (ePHI) protections, but is alleged as vague and lax in enforcement (Hoffman & Podgurski 2007). Moore and Frye (2019) state that HIPAA compliance is not only "technical safeguards" but also continuing administrative controls. Even with these mandates, breaches are all too common. Ahmed et al. (2025) demonstrate that ransomware campaigns crippled U.S. hospitals, leading to large delays in care, highlighting the inadequacy of HIPAA for resilience.

To complement HIPAA, HHS released 405(d) Health Industry Cybersecurity Practices (HICP), which lists the top five challenges (phishing, ransomware, insider threats, theft, and medical device risk) in relation to approachable advice on how they can be mitigated (Chua & Pmp, 2021). The Food and Drugs Authority's (FDA) Cybersecurity in Medical Devices guidance includes an enforcement checklist that manufacturers are required to abide by, including building security into the design and submitting software bills of materials (SBOMs). Comparative works point for differences: U.S. FDA guidance focuses on lifecycle cybersecurity, whereas Europe's Medical Device Coordination Group (MDCG) approach continues non-prescriptive (Skytterholm *et al.,* 2025). Freyer et al. (2024) also demonstrate and report that, overall, in the U.S., EU and Asia-Pacific, cybersecurity of medical devices is not consistently integrated into benefit-risk evaluations.

Policy momentum is accelerating. U.S. regulators proposed new rules late in 2024 to toughen up data protection requirements for the health sector, highlighting the continuing evolution of compliance there.

Energy and Utilities

The U.S. energy industry is regulated by the NERC CIP, which carries a legal weight under the authority of FERC. CIP-013-3 (2023) requires that the operators of the Bulk Electric System have programs in place to manage supply chain risk. CIP-015-1 (2025) introduces requirements for internal network security monitoring to cover advanced operational transformation intrusion threats. Resources such as the NERC CIP glossary published by Fortinet assist non-experts in understanding these controls. Finally, a July 2025 FERC cybersecurity order is an indication of regulatory action tightening around bulk electric system resilience.

NIST guidance complements these standards. SP 800-82 (Incident Command System (ICS) security) and SP 800-161r1-upd1 (C-SCRM) also directly applies to operational transformation, with technical controls as well as procurement-oriented compliance templates being incorporated into the document (Boyens *et al.,* 2022). By mandating that entities document policy, risk appetite and roles at an enterprise level, a mission level and then in the actual (operational) space, SP 800-161 guarantees compliance activities are built-in during the entire lifecycle of operational transformation systems. As Chatterjee (2021) observes, supply chain malware use in the oil and gas industry emphasizes the need for these standards; occurrences such as Solar Winds demonstrate that security weaknesses are not limited to a single sector.

Public Sector and Cross-Sectoral Compliance

Public administration is burdened by mandates to adhere to, these mandates cut across various critical services. In the U.S., OMB's M-22-09 obligates agencies to complete certain Zero Trust best practices with procurement, identity and encryption milestones. CISA's ZTMM v2. 0 defines and strengthens these goals by providing measurable levels of measures to be achieved in the five pillars (CISA, 2023). In the European Union, Directive NIS2 extends the number of types of entities required to comply, shortens the timeframes for reporting breaches and applies material fines for noncompliance (Singh, 2023).

The other substantial EU regulation, the Cyber Resilience Act (CRA) that entered into force in December 2024, mandates cybersecurity standards for all digital components. Requirements will be effective from December 2027, and the products must be Conformité Européenne **(**CE) marked to show conformance (European Commission, 2024). As Chiara (2022) puts it, the CRA brings in horizontal regulation whereby compliance is no longer limited to the sectoral silos but applies across the entire spectrum of digital products. This is a move toward preventative regulation, turning secure-by-design into something that companies must do instead of only a best practice.

Cross-Cutting Compliance Challenges

Numerous compliance hurdles exist across industries. First, regulatory fragmentation makes cross-border operations more difficult. Companies must reconcile HIPAA with General Data

Publisher: SARC Publisher

Protection Regulation (GDPR) or NERC CIP with energy regulations in the EU. Second, enforcement is still patchy, criticizing HIPAA as a toothless law while NIS2 and DORA place great obligation on national supervisory capability. Third, there is always a time lag between the adoption of technology and the implementation requirements. As Feliciano-Cestero et al. (2023) note, digital transformation is constrained by fragmented regulatory regimes and inadequate enforcement. This tension between innovation and compliance is the paradox that underlines digital censorship.

The compliance frameworks examined show that there is strong sectoral coverage, especially in the financial and energy sectors where there is a well-defined enforcement mechanism. However, the healthcare and cross-border situations reveal the weakness of fragmented regulatory regimes. The merit of the EU strategy is that it is legally binding, and the U.S. model is more inclined to flexibility through guidance. Striking a balance between these two orientations: rigor and adaptability is a burning issue in the harmonized global compliance.

TECHNOLOGY-ENABLED PRACTICES FOR SECURITY

Technology enables both digital transformation (DT) in regulated industries, and at the same time constitutes the leading vector for new threats. Secure advancement is only possible by adding security to technologies, practices and architectures in design through deployment. All around the country and world, entities follow frameworks such as the NIST Secure Software Development Framework (SSDF), OWASP Software Assurance Maturity Model (SAMM), Zero Trust infrastructures, and supply-chain risk management principles. These frameworks aim to implement the obligations of compliance as technical and organizational measures.

Secure Software Development and DevSecOps

The foundation of secure DT is software integrity. The NIST SSDF (Society for Software Quality) provides a core set of high-level secure software development practices that organizations can implement within their SDLC (Souppaya *et al.,* 2022). Acts involve specifying security requirements, securing the development environment, ensuring code correctness, and vulnerability handling. Most importantly, SSDF guidance is outcome-oriented instead of being prescribed and therefore flexible across sectors.

Recent extensions underscore the state-of-the-art. NIST SP 800-218A (2024) is adapted to SSDF for generative AI and dual-use foundation models garmenting safeguards around model weights, pipelines as well as reward functions (Booth, *et al.,* 2024). This is symptomatic of the use of AI in healthcare diagnostics, financial fraud detection and energy optimization amongst others where AI weaknesses could propagate down to a regulated service. Thus, SSDF and its AI profile inject secure-by-design into conventional as well as the new DT technology.

Industry frameworks complement NIST guidance. OWASP SAMM is assessed in financial domains where it offers a maturity model process to measure with secure development life cycle adoption (Fucci *et al.,* 2024). By matching security approaches with a company's own level of maturity, SAMM can be used by regulated entities to track progress, uncover emerging gaps and make the case for investing in DevSecOps. This staged maturity assessment guarantees that it's not just security but improving security.

Zero Trust Architectures

Over the past decade, Zero Trust (ZT) has become an architectural security model for protecting DT. Zero Trust (ZT), as described in NIST SP 800-207, represents an architectural paradigm for safeguarding DT environments. Rather than assuming implicit trust in users or devices, ZT enforces continuous verification of access requests by evaluating identity, device posture, and contextual attributes. OMB M-22-09 requires federal agencies to comply with ZT no later than FY2024, it is now an essential public sector compliance issue. To help enable this, CISA's Zero Trust Maturity Model v2. 0 provides an incremental roadmap through five pillars which are Identity, Devices, Networks, Applications/Workloads and Data supported by governance, visibility, and automation (CISA, 2023).

Academic research reinforces practical challenges. Yeoh et al. (2023) determines that organization sponsorship, automation and culture are critical success factors for Zero Trust implementation. The Massachusetts Institute of Technology (MIT)/U.S. Department of Homeland Security (DHS) Zero Trust architecture report (2020) extends this analysis further by contrasting ideas like Software-Defined Perimeter (SDP) and Google's BeyondCorp, discussing the trade-offs of being so strict in implementation for federal and regulated

Publisher: SARC Publisher

environments (Uttecht, 2020). These assets together don't present Zero Trust as a static list of controls, but as a dynamic architecture that needs governance, culture and technology to be in place.

Cloud Security and Compliance

Cloud migration is a key focus of DT, but regulated industries need to take that step under strong security premises. U.S. agencies adhere to Federal Risk and Authorization Management Program (FedRAMP) baselines which are transparent about cloud service provider authorizations. In the UK, essential service providers are also directed by the National Cyber Security Centre's (NCSC) Cyber Assessment Framework (CAF) to in-source compliance with cloud and digital services. Although the FFIEC AIO Handbook (2021) accepts the inevitability of cloud adoption and advises that institutions focus on ensuring that cloud usage is consistent with resilience, Zero Trust, and board-level oversight (Council, 2021).

CISA's Cloud Security Technical Reference Architecture, which is incorporated into the ZTMM additionally helps ensure agencies moving to the cloud implement least privilege, encryption, and secure configuration as a built-in rather than bolted on (CISA, 2023). These cloud-specific compliances agents collectively turn governance into technology constraints on DT.

Supply Chain Security and Assurance

One of the largest potential threats to DT is supply-chain vulnerabilities. NIST SP 800-161r1-upd1 (2022; updated 2024) describes C-SCRM as a discipline and practice to effectively manage supply chain risk; it is a systematic process for managing exposure to cybersecurity risk while optimizing supply chain decision (Boyens *et al.,* 2022). It mandates that organizations incorporate supplier risk assessment into enterprise risk management, establish acquisition policy and maintain customized C-SCRM plans at the enterprise, mission/business processes, and system levels. The standard gives templates, control catalogs and measurement subjects to make supply chain assurance auditable and repeatable.

Sectoral standards enforce supply-chain practices. In the energy sector, NERC CIP-013-3 mandates that utilities evaluate and manage risks in vendor acquisitions and patching (CIP-013-3, 2023). Chatterjee (2021) brings home the stakes by examining malware compromises within oil and gas supply chains, concluding that events like SolarWinds illustrate how third-party weaknesses can spill over into critical infrastructure. With SBOM obligations and third-party accountability embedded, supply chain security shifts from best practice to legally mandated compliance.

Integrating Technology Practices Across Sectors

In all, these frameworks suggest a direction where technology-enabled practices are moving toward secure-by-design principles. SSDF facilitates secure development, SAMM measures maturity, Zero Trust architectures reset access and perimeter, FedRAMP/CAF pushes cloud security adoption and SP 800-161 institutionalizes supply-chain confidence. Academic reviews like Saeed et al. (2023), argue that while DT enhances efficiency, it amplifies attack surface, thereby requiring cyber risk management framework, which interlocks compliance, technology and governance.

Technology frameworks all develop the philosophy of secure-by-design. SSDF and OWASP SAMM offer scalable approaches to integrating security into development cycles, and Zero Trust architectures offer quantifiable maturity approaches. Their weakness is the complexity of implementation and organizational preparedness; they cannot succeed without a steady adoption of the system, resources, and culture change among regulated parties.

Human and Organizational Factors

Governance, compliance, and technology serve as structural enforcers, but a secure DT is based on human and organizational dynamics. Regulated industries continue to struggle to establish a security culture, infuse awareness into the tactics of everyday business and better align leadership responsibility with regulatory scrutiny. Studies in health care, finance and government all underline that resilience directly depends on organizational culture and practices of employees, alongside managerial attitudes, not only technical safeguards.

Security Culture and Awareness

DT security outcomes continue to be strongly influenced by organizational culture. Nowicka et al. (2024) stated that information security management should be considered a condition for the operation of the organization, making it clear that compliance needs an integrated project including audit, awareness and managerial support. This is a move away from treating cybersecurity as

Publisher: SARC Publisher

an IT task to integrating it into every business process.

For example, in health care, the HHS 405(d) Health Industry Cybersecurity Practices framework highlights employee awareness and rates phishing, ransomware, and negligent behavior as the top threats (Chua & Pmp, 2021). This being in the top five threats demonstrates that human behavior has a direct impact on regulated entities. Feliciano-Cestero et al. (2023) reinforce this point, highlighting that cultural adaptation failures in the form of inadequate training or reaction against new processes can have serious implications for the success of DT initiatives.

Insider Risk and Error Humans

Human error and insider threat are ongoing in compliance regimes but represent major risks. Hoffman and Podgurski (2007) criticized the HIPAA Security Rule for providing dilute imperatives concerning insider risk, noting that its flexible language did not clearly specify operational precautions. Recent US health care related breaches validate such deficiencies as Ahmed *et al.,* (2025) indicate that compromised vendor accounts and carelessness was often involved before a ransomware attack.

Insider risks continue to haunt users in the energy and OT sectors. Chatterjee (2021) emphasizes that many of the compromises in oil and gas supply chains via malware were associated with human errors, such as failures to patch systems or checkup vendor access. Taken together, these results reveal that compliance frameworks which require technical controls must include behavioral measures including role-based training and continuous monitoring for privileged users.

Leadership and Accountability

The commitment of leadership is critical in connecting policy and practice. The NIS2 Directive provides an example of such imposing management bodies with personal liability for cybersecurity failures in EU-regulated sectors, thus treating cyber risk as a matter of board-level responsibility. Other U.S. governance frameworks, like OMB M-22-09 and NIST SP 800-161r1-upd1 stress that senior executives should approve strategies, define a risk appetite and direct supply-chain risk management (Boyens *et al.,* 2022). Without a top-down commitment, policies yield to under enforcement and cultural change grinds to a halt.

Research demonstrates that leadership buy-ins frequently the missing piece. Saeed *et al.,* (2023) revealed or rather discovered that, although organizations invested in advanced technology, it was yet to be supported by top management to ensure common cybersecurity practices. This leadership deficiency can result in organizations that are technically sophisticated yet operationally soft.

Change Management in Transformation

Secure DT in the real world must overcome organizational push-back to change. Stoumpos *et al.,* (2023) emphasized that e-health technologies encounter resistance in the health sector due to technical and human-related impediments. Adıgüzel (2025) also highlights that next generation banking is not simply about regulatory fit but also a shift in culture where staff have to integrate AI, cloud and blockchain systems within existing processes. These examples demonstrate that security compliance frameworks work only when they are combined with business change and technical implementation.

The human, but also organizational factors are widely underestimated in secure DT. Culture, insider risk, leadership and change management weaknesses can undercut the most innovative governance and compliance programs. Although regulations such as HIPAA, FFIEC, and NERC CIP set guidelines for structure, you can't simply make security part of your daily routine without ongoing awareness messaging that drives culture change, accountability from senior staff to leadership to end users. As Feliciano-Cestero et al. (2023) have argued, the outcomes of DT are not just reliant on technology savviness but also human adaptability to new processes.

Human-centric strategies provide a much-needed yet not always considered dimension to ensure change. The best thing about the existing frameworks is their increasing recognition of culture, awareness and leadership as resilience drivers. Nevertheless, they are poorly operationalized in most compliance models, which implies that behavioral aspects of cybersecurity are not adequately gauged or rewarded.

IMPLEMENTING RESILIENCE AND RISK MANAGEMENT

Resilience has become the central yardstick for digital transformation (DT) in regulated sectors (Kahan *et al.,* 2009). Governance creates the structures and compliance enforces the mandates,

Publisher: SARC Publisher

while resilience and risk management help organizations to anticipate, absorb and respond to disruptions. From finance and healthcare to energy and public service, resilience is becoming ever more encoded in regulation, operationalized through testing, and positioned in enterprise endeavor.

Conceptual Foundations of Resilience

The resilience frameworks emphasize flexibility instead of static adherence. Kahan *et al*. (2009) draw from the concept of resilience to be an ability to shield, absorb, and renew activities following disruptions (2009). This operational paradigm has shaped U.S. homeland security policy and still informs sectoral strategies. Saeed *et al*. (2023) move this concept further to digital transformation and maintain that cybersecurity resilience should be inbuilt in DT efforts to mitigate risks like data leakages and cyber-attacks.

FINANCIAL SECTOR RESILIENCE

Some of the clearest evidence of resilience by design can be found in financial services. The Basel Committee Principles for Operational Resilience (2021) demand that banks have in place effective governance, ICT continuity, third-party oversight and incident response capabilities (Supervision, 2021). In the U.S., the FFIEC IT Handbook AIO (2021) similarly directs institutions to embed resilience by aligning infrastructure, operations, and governance to withstand cyber incidents (Council, F. F. I. E. 2021). Leo (2020) demonstrates that global systemically important banks (G-SIBs) disclosed resilience activities in annual reports have been uneven, thus revealing that gaps existed between regulatory requirements and transparency. Taken together, these studies validate financial resilience as being more than a technical necessity, it is a compliance obligation with market-wide ramifications.

The Digital Operational Resilience Act (DORA), adopted by the EU, sets out a model for breaking down silos by introducing binding requirements of ICT risk management, incident reporting and stress tests across the financial industry. The official text mandates all firms under its regulation to include resilience in governance, and supply-chain oversight, adapting these into practice is the work of supervisory bodies such as EIOPA (European Commission, 2024).

Healthcare Sector Resilience

In health care, resilience should not only focus on patient safety but also on service continuity. Ahmed *et al*. (2025) describe how ransomware attacks disrupted patient care, highlighting the insufficiency of compliance-oriented frameworks such as HIPAA. On the contrary, additional efforts such as HHS 405(d) Health Industry Cybersecurity Practices focus on resilience by recommending multilayered defense against the top five threats (Chua & Pmp, 2021). Freyer *et al*. (2024) mention an enduring bias in the regulation of medical devices, reflected by their finding that cybersecurity is not uniformly incorporated into benefit-risk assessments and that measures to enhance resilience are disorganized. In combination, these pieces of work demonstrate that health care resilience is about the balance between regulatory compliance and operational preparedness.

Energy and Infrastructure Resilience

Resilience is not just structural; energy system resilience embodies this concept as a national security priority. The NERC CIP standards formalize the resilience of the bulk electric system. CIP-013-3 (2023) dictates lifecycle risk management programs, CIP-015-1 (2025) demands internal monitoring to watch for lateral movement and operational technology environment intrusions. Those compliance efforts are backed by FERC's cybersecurity order 2025 announcement, which increased resilience requirements for utilities that serve critical grid infrastructure. NIST's guidelines supplement these in sectorial and industry specific standards: SP 800-161r1-upd1 incorporates supply-chain resilience into enterprise risk management, with the central notion that "ownership and accountability for cybersecurity risks within the supply chain resides ultimately with the head of an organization" (Boyens *et al.,* 2022).

Chatterjee (2021) explains the ramifications, demonstrating that malware attacks in OT supply chains of oil and gas led to production disruptions and increased systemic risks. These instances underscore the fact that resilience is built on visible proactive supply chain assurance and monitoring, not just compliance audits.

Public Sector and Multi-Sectoral Resilience

In the public sector, resilience is explicitly related to trust in government services. According to OMB M-22-09 and CISA's Zero Trust Maturity Model, agencies will not be able enumerate operational resilience gains without a fundamental re-architect of identity, network, and data protection (CISA, 2023). In the EU, NIS2 extends

Publisher: SARC Publisher

resilience requirements to critical and essential entities, with breach reporting timeframes as low as 24 hours (Singh, 2023). This last point is extended even further under the Cyber Resilience Act (CRA) which requires lifecycle security for all products that contain digital features, by embedding resilience into the consumer-connected technology environment (European Commission, 2024).

Persistent Challenges

Although there has been progress in regulation, building resilience remains a challenge. Multinational companies must duplicate efforts to comply with fragmented requirements between jurisdictions. Requirements for disclosure also continue to be uneven, hobbling accountability, as Leo (2020) demonstrates. Healthcare remains weak in cybersecurity, with breaches that inevitably impact service despite decades of HIPAA enforcement. In energy, regulatory incrementality might still slip further behind adversary innovation. Lastly, AI-enabled DT-resilience is an under-researched area, though technical guidance for NIST's SSDF-AI profile has paved the way, governance and compliance schemes around resilience of AI are still emerging (Booth *et al.,* 2024).

Resilience is no longer a desired situation, but a minimum requirement in all regulated parts of the economy. You see it in financial regulators including it into operational resilience standards; healthcare frameworks increasingly focusing on continuity of care; energy regulations codifying supply-chain assurance and public sector edicts pushing Zero Trust adoption. But clear holes remain, particularly in enforcement, transparency and AI governance. Bridging these gaps is necessary if digital transformation is to become secure and sustainable.

DISCUSSION

Secure DT in regulated industries is a function of governance, compliance, technology and organization. The discussion on U.S. and international framing shows that there is a commonality in shared principles, including resilience, secure-by-design engineering, accountability, as well as divergence with respect to legal traditions of law-making/thinking, sectoral foci and enforcement capacity. This debate critically reflects on cross-sectoral evidence, highlighting conceptual trends, practical frontiers and policy implications.

Convergence Around Core Principles

Some of these principles are common across jurisdictions underpinning DT security. The first is resilience, where U.S. regulators stress the importance of operational resilience in banking (FFIEC, Basel Committee), continuity of care in healthcare (HHS 405(d)), and supply-chain monitoring in energy (NERC CIP-013-3, CIP-015-1) (CIP-013-3, 2023). DORA of the EU writes this into law, so resilience becomes mandatory across financial services. NIS2 requires incident response and reporting for critical entities too, and the Cyber Resilience Act (CRA) extends lifecycle resilience to consumer products (European Commission, 2024).

The second is secure-by-design. NIST's SSDF, its AI extension (Souppaya *et al.,* 2022; Booth *et al.,* 2024), and OWASP SAMM institutionalize: practices that move responsibility for security upstream in the development lifecycle (Fucci *et al.,* 2024). The CRA then adds an extra layer to this by requiring life-cycle security obligations on producers, with CE Marking serving as evidence for its fulfillment.

The third is Zero Trust. Both the U.S. and EU approaches focus on moving past perimeter defenses. The U.S. operationalizes this via OMB M-22-09 and CISA's Zero Trust Maturity Model v2. 0, that agencies accomplish against CISA (2023). Literature indicates that the approach to Zero Trust adoption is influenced by automation, culture adjustment and executive buy-in (Yeoh *et al.,* 2023). It mirrors a worldwide understanding that change can't depend on trust and unchanging controls.

Divergence of U.S. and EU Strategies

While both adhere to the principle of the rule of law, U.S. and EU compliance models are not convergent. The American approach is a composite of frameworks and sector regulation. NIST SP 800-161r1-upd1 incorporates supply-chain security into enterprise risk management though it is only voluntary within the federal government. (Boyens *et al.,* 2022). Industry-sector mandates such as HIPAA, NERC CIP and FFIEC guidance create pockets of coverage, but enforcement is mixed. HIPAA, for instance, has been accused of being overly ambiguous and lenient in terms of fines owed by those caught disrupting healthcare with ransomware (Hoffman & Podgurski, 2007; Ahmed *et al.,* 2025).

Publisher: SARC Publisher

The EU model, by contrast, incorporates enforcement in binding law itself. NIS2 and DORA hold management personally responsible and streamline responsibilities among member states. The CRA extends the same obligations to all digital products, not just essential ones (Chiara, 2022). This mirrors a regulatory mindset that considers cybersecurity to not be just a sectoral or national security, but also a consumer protection and market integrity issue. But enforcement capability is uneven in member states, so it is not clear how harmonized in practice we can be.

Sectoral Contrasts

Sectoral differences also shape compliance. Finance is leading the way: Basel, DORA, FFIEC and operational resilience standards layer obligations that are internationally synchronised (Supervision, 2021). There is fragmented healthcare because HIPAA provides mere floor, augmented by HHS 405(d), FDA device guidance and proposed HHS rules, yet epidemics of breaches (Chua & Pmp, 2021; Skytterholm *et al.,* 2025; Ahmed *et al.,* 2025). Energy compliance is codified through legally enforceable NERC CIP standards; however, these only address OT and may leave other ICT/IoT vulnerabilities largely unaddressed (Chatterjee 2021). Public sector requirements like OMB M-22-09 drive adoption of aggressive Zero Trust in that if we can mandate those controls here, maybe they should be implemented everywhere.

The reviewed frameworks demonstrate a powerful movement towards risk-based, adaptive forms of governance. Their greatest advantage is that they offer modular guidance that can be customized to sectoral contexts. Nevertheless, their comparability and effectiveness in the long term are limited due to the lack of common performance metrics and their unequal application across jurisdictions.

Persistent Gaps

Despite advances, gaps remain. Regulatory fragmentation wrenches multinational companies through overlapping regimes such as HIPAA and GDPA for healthcare, NERC CIP and CRA/NIS2 for energy. Inequity creates a lack of deterrence. HIPAA penalties are weak, but NIS2 fines can go as high as €10M or 2% of the worldwide turnover (Singh, 2023). Even with detailed guidelines from the NIST SP 800-161r1-upd1, assuring supply-chain remains a challenge, as transparency in multi-tier vendor systems is minimal (Boyens *et al.,* 2022). Finally, AI governance is underdeveloped. In addition to practices from NIST SSDF-AI, legal regime and compliance of AI resilience as an end-to-end system need to catch up (Booth *et al.,* 2024).

Implications

These discontinuities and gaps indicate that in a regulated DT world perhaps the most pragmatic path to secure DT may lie somewhere in between voluntary approaches like NIST CSF and SSDF which provide technically flexible guidelines, balanced with regulatory models like DORA or NIS2 for liabilities. Cross-industry cooperation is crucial, and this is especially so for supply-chain assurance and AI governance. Without that, DT may wind up reinforcing sectoral silos and regulatory contradictions that adversaries can readily exploit.

RESEARCH GAPS AND FUTURE DIRECTIONS

While governance compliance, technology and organizational aspects are becoming more codified in Secure Digital Transformation practices, research and regulatory papers expose ongoing discrepancies. Solutions to these are critical for a robust, secure and trustworthy transformation into regulated domains.

Fragmented and Overlapping Regulations

One of the main gaps is regulatory fragmentation, notably for multinationals. Healthcare companies are forced to balance HIPAA with GDPR Article 32, which requires appropriate technical and organizational measures for security (Hoffman & Podgurski, 2007; Selzer *et al.,* 2021). Inversely, the NERC CIP standards may apply to energy operators in the U.S. while preparing for EU's NIS2 and CRA, (European Commission, 2024; CIP-013-3, 2023). Researchers like Feliciano-Cestero *et al*. (2023) add that these fragmented regimes are a threat to the feasibility of DT because they introduce compliance cost and uncertainty, thus increasing legal risk. Future work can be devoted to examining these cross-regulatory harmonization frameworks and interoperable compliance metric systems.

Enforcement and Accountability Gaps

Even where they exist, enforcement is uneven. The enforcement of HIPAA has been largely lax, and this vagueness in requirements is said to offer little deterrence against negligence (Hoffman & Podgurski, 2007). Conversely, NIS2 fines for non-compliance up to €10 million or 2% of turnover (Singh, 2023). This gap in coverage leads to questions about the role of penalties on compliance

Publisher: SARC Publisher

across sectors. More research to compare enforcement effectiveness, particularly in health care and critical infrastructure, is needed.

Supply Chain Assurance

Cloud supply chain assurance is constrained by visibility gaps and vendor intransparency notwithstanding detailed specifications such as NIST SP 800-161r1-upd1 and NERC CIP-013-3 (Boyens *et al.,* 2022; CIP-013-3, 2023). Chatterjee (2021) reveals that security challenges associated with supply-chain malware within the OT sector remain in place, even in rigid circumstances. Future work should focus on multi-tier vendor transparency, operationalization of SBOM; automated risk monitoring, particularly in light of AI-based supply chain analytics development.

Human and Organizational Dimensions

Human factors are persistently under-researched. Although insider threats and employee carelessness are emphasized in HHS 405(d), many compliance schemes concentrate on technical safeguards (Chua, & Pmp, 2021). According to Hoffman and Podgurski (2007), vague compliance requirements ignore the reality of organizational operations. Saeed et al. (2023) suggest that, while not being the weakest link, leadership buy-in and cultural adaptation are frequently overlooked. In the future, possible research within this direction might be compliance in behavioral economics, cultural obstacles to Zero Trust adoption, and leadership responsibility in DT.

AI and Emerging Technologies

The regulation of AI in regulated industries is still in its infancy. NIST SP 800-218A enhances SSDF with AI-specific practices, however, there is currently no overarching regulation dealing with resilience or accountability in AI-driven DT (Booth *et al.,* 2024). Mauro et al. (2024) and Stoumpos et al. (2023) demonstrated new governance and security challenges as an outcome of AI and IoT adoption in healthcare. Next, research should investigate models of compliance tailored to AI that appropriately quantify the risk of those systems based on AI and govern themselves around sectorial regulations.

Metrics and Benchmarking

Finally, there is a shortage of strong success criteria for secure DT. Although required to disclose by FFIEC and Basel, the reporting of banks' operational resilience has so far been found as inconsistent (Leo, 2020). Without standardized metrics, it is challenging to gauge relative progress against other sectors or geographic areas. Work on cross-sector KPIs for resilience, compliance maturity and cultural alignment is lacking.

Challenges ahead are how to tackle regulatory fragmentation, enforcement vacuum, supply chain guarantee and human factors in secure DT research as well as AI governance and benchmarking. Without progress in these areas, regulated sectors could well end up with fragmented point solutions that satisfy the compliance obligation but do not deliver resilience in reality. By leveraging models such as NIST SSDF, CISA's Zero Trust models and EU's DORA/NIS2, future research will evolve into an integrated, cross-sectoral and quantifiable method for securing digital transformation.

CONCLUSION

Trusted DT in the regulated sectors is crucial for sustaining trust as technologies evolve at a faster pace and cybersecurity threats escalate. This review examined governance regimes, regulatory requirements, technological innovations, organizational predictors and resilience models at the U.S. level and beyond. Even though governance philosophies are different (US with flexible requirements: NIST CSF 2.0, SSDF, CISA ZTMM vs the EU with regulatory mandates: NIS2 DORA CRA), both end up on resilience as the central principle. But it is organization culture, leadership and human factors which will continue to be indecisive, with lingering holes in supply-chain assurance, enforcement and AI governance. True resilience will take a hybrid systems approach, encompassing secure-by-design frameworks, legal obligations for accountability, organizational cultures of awareness and strategic resilience that embrace bumpy rides. It is only through this incorporation that regulated sectors will be able to shift from compliance to secure, sustainable digital ecosystems.

REFERENCES

1. Adıgüzel, İdris. "New Generation Banking: A Conceptual Framework for Digital Transformation in the Financial Sector." (2025).
2. Ahmed, Z., Osifowokan, A. S., Filani, A., and Donkor, A. A. "Comprehensive Analysis of Cyber-Attacks and Data Breaches in the US Health Sector: Identifying Vulnerabilities and Developing Proactive Defense Strategies." (2025).
3. Booth, H., Souppaya, M., Vassilev, A., Ogata, M., Stanley, M., and Scarfone, K. "Secure Software Development Practices for

Publisher: SARC Publisher

Generative AI and Dual-Use Foundation Models: An SSDF Community Profile." (2024).
4. Boutin, C. "NIST Releases Version 2.0 of Landmark Cybersecurity Framework." (2024).
5. Boyens, J., Smith, A., Bartol, N., Winkler, K., Holbrook, A., and Fallon, M. *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.* NIST Special Publication 800-161 upd1 (2022).
6. Chatterjee, S. "Mitigating Supply Chain Malware Risks in Operational Technology: Challenges and Solutions for the Oil and Gas Industry." *Journal of Advanced Development Research* 12.2 (2021): 1–12.
7. Chiara, P. G. "The Cyber Resilience Act: The EU Commission's Proposal for a Horizontal Regulation on Cybersecurity for Products with Digital Elements: An Introduction." *International Cybersecurity Law Review* 3.2 (2022): 255–272.
8. Chua, J. A., and Pmp, C. "Cybersecurity in the Healthcare Industry." *Physician Leadership Journal* 8.1 (2021): 69–72.
9. CIP-013-3. *Cyber Security – Supply Chain Risk Management.* NERC (2023).
10. Council, F. F. I. E. *FFIEC Information Technology Examination Handbook: Architecture, Infrastructure, and Operations.* Federal Financial Institutions Examination Council (2021).
11. Cybersecurity and Infrastructure Security Agency (CISA). *Zero Trust Maturity Model Version 2.0.* (2023).
12. European Commission. *NIS2 Directive: Securing Network and Information Systems.* (2024).
13. European Commission. *Cyber Resilience Act.* (2024).
14. European Insurance and Occupational Pension Authority (EIOPA). *Digital Operational Resilience Act (DORA).* (2025).
15. Feliciano-Cestero, M. M., Ameen, N., Kotabe, M., Paul, J., and Signoret, M. "Is Digital Transformation Threatened? A Systematic Literature Review of the Factors Influencing Firms' Digital Transformation and Internationalization." *Journal of Business Research* 157 (2023): 113546.
16. Freyer, O., Jahed, F., Ostermann, M., Rosenzweig, C., Werner, P., and Gilbert, S. "Consideration of Cybersecurity Risks in the Benefit-Risk Analysis of Medical Devices: Scoping Review." *Journal of Medical Internet Research* 26 (2024): e65528.
17. Fucci, D., Alégroth, E., Felderer, M., and Johannesson, C. "Evaluating Software Security Maturity Using OWASP SAMM: Different Approaches and Stakeholders' Perceptions." *Journal of Systems and Software* 214 (2024): 112062.
18. General Data Protection Regulation (GDPR). *GDPR Article 32.* (2025).
19. Hoffman, S., and Podgurski, A. "Securing the HIPAA Security Rule." *Journal of Internet Law* (2007): 6–26.
20. Kahan, J. H., Allen, A. C., and George, J. K. "An Operational Framework for Resilience." *Journal of Homeland Security and Emergency Management* 6.1 (2009).
21. Leo, M. "Operational Resilience Disclosures by Banks: Analysis of Annual Reports." *Risks* 8.4 (2020): 128.
22. Mauro, M., Noto, G., Prenestini, A., and Sarto, F. "Digital Transformation in Healthcare: Assessing the Role of Digital Technologies for Managerial Support Processes." *Technological Forecasting and Social Change* 209 (2024): 123781.
23. Moore, W., and Frye, S. "Review of HIPAA, Part 1: History, Protected Health Information, and Privacy and Security Rules." *Journal of Nuclear Medicine Technology* 47.4 (2019): 269–272.
24. NERC CIP Standard. "Key Compliance Requirements, Challenges, and Best Strategies." (2024).
25. Giannasca, Nicholas A. "What Energy Sector Stakeholders Should Know About the New Standard to Further Protect the Nation's Bulk Electric System." (2025).
26. Nowicka, J., Ciekanowski, Z., and Milewska, A. "Information Security Management as the Basis for the Functioning of an Organization." (2024).
27. Regulation (EU) 2022/2554. *Digital Operational Resilience for the Financial Sector.* European Parliament and Council (2022).
28. Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., and Alabbad, D. A. "Digital Transformation and Cybersecurity Challenges for Business Resilience: Issues and Recommendations." *Sensors* 23.15 (2023): 6666.
29. Selzer, A., Woods, D., and Bohme, R. "An Economic Analysis of Appropriateness under Article 32 GDPR." *European Data Protection Law Review* 7 (2021): 456.

Publisher: SARC Publisher

30. Singh, C. "The European Approach to Cybersecurity in 2023: A Review of the Changes Brought in by the Network and Information Security 2 (NIS2) Directive 2022/2555." *International Company and Commercial Law Review* 5 (2023): 251–261.
31. Skytterholm, A. N., Androutsos, C., Ntanis, A., and Jaatun, M. G. "Cybersecurity Guidances for Medical Devices: An MDCG and FDA Regulatory Comparison." In *Proceedings of the IEEE International Conference on Smart Computing (SMARTCOMP)* (2025): 336–341.
32. Souppaya, M., Scarfone, K., and Dodson, D. *Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities.* NIST SP 800-218 (2022).
33. Stoumpos, A. I., Kitsios, F., and Talias, M. A. "Digital Transformation in Healthcare: Technology Acceptance and Its Applications." *International Journal of Environmental Research and Public Health* 20.4 (2023): 3407.
34. Basel Committee on Banking Supervision. *Principles for Operational Resilience.* (2021).
35. Uttecht, K. D. *Zero Trust (ZT) Concepts for Federal Government Architectures.* (2020).
36. Davis, Wes. "The US Proposes Rules to Make Healthcare Data More Secure." *The Verge* (2024).
37. Yeoh, W., Liu, M., Shore, M., and Jiang, F. "Zero Trust Cybersecurity: Critical Success Factors and a Maturity Assessment Framework." *Computers & Security* 133 (2023): 103412.
38. Young, S. D. *Moving the US Government toward Zero Trust Cybersecurity Principles.* Memorandum M-22-09 (2022).

Source of support: Nil; **Conflict of interest:** Nil.

Cite this article as:
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.

Publisher: SARC Publisher