World Journal of Advanced Research and Reviews

eISSN: 2581-9615 CODEN (USA): WJARAI

Cross Ref DOI: 10.30574/wjarr

Journal homepage: https://wjarr.com/

(Review Article)

Balancing efficiency and security: The role of voluntary standards and emerging technologies in cyber risk management framework in USA perspective

CHISOM ELIZABETH ALOZIE [1, *] and UZOAMAKA OKAFOR [2]

[1] *Department of Information Technology Institution, University of the Cumberlands, Kentucky, United States.*

[2] *Department: Satish and Yasmin Gupta College of Business-Center for Cybersecurity Institution: University of Dallas, Irving, Texas, USA.*

World Journal of Advanced Research and Reviews, 2025, 26(02), 1746-1776

Publication history: Received on 03April 2025; revised on 09 May 2025; accepted on 11 May 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.26.2.1842

Abstract

This research examines the distinctive evolution of voluntary cyber risk management frameworks within the United States context, focusing on the tension between security imperatives and operational efficiency. Through a mixed-methods approach combining 37 interviews with U.S. chief information security officers, regulatory experts, and framework architects, alongside survey data from 156 U.S. organizations, this study identifies unique characteristics of the American approach to cyber risk management. Findings reveal that U.S. organizations demonstrate distinctive patterns in framework utilization, prioritizing sector-specific adaptations and legal risk management considerations while leveraging emerging technologies to automate compliance activities. The research identifies a "federated implementation model" prevalent among U.S. enterprises that balances central governance with business unit autonomy. The study contributes a novel "USA Cyber Risk Integration Framework" that accounts for the sectoral regulatory landscape, litigation-aware governance structures, and technology-driven compliance approaches characteristic of U.S. organizations. This research provides valuable insights for security practitioners, technology vendors, and policymakers seeking to understand and enhance cyber risk management effectiveness within the unique American regulatory and business environment.

Keywords: Cyber Risk Management; Nist Cybersecurity Framework; Us Regulatory Landscape; Security Automation; Compliance-Driven Governance; Sector-Specific Standards; Public-Private Partnerships

1. Introduction

1.1. The Evolution of Cyber Risk Management in the U.S. Context

The United States represents a distinctive environment for cyber risk management, shaped by its historical emphasis on market-driven solutions, sectoral regulatory approach, and litigation-oriented business culture. Unlike jurisdictions that have implemented comprehensive cybersecurity legislation, the U.S. has historically relied on a combination of sector-specific regulations, voluntary frameworks, and market incentives to drive cybersecurity improvements (Wolff, 2018). This approach reflects broader American governance preferences for flexibility, innovation, and minimal government intervention in private-sector decision-making.

The evolution of U.S. cyber risk management has been significantly influenced by several pivotal developments. The 9/11 attacks prompted increased focus on critical infrastructure protection, leading to initiatives like the National Infrastructure Protection Plan. The massive Target data breach in 2013 elevated cybersecurity to a board-level concern, introducing new expectations for executive oversight (Bamberger & Mulligan, 2019). Executive Order 13636 in 2013

[*] Corresponding author: CHISOM ELIZABETH ALOZIE

directed the National Institute of Standards and Technology (NIST) to develop a voluntary Cybersecurity Framework, establishing what would become the most influential framework in the American context.

Table 1 Evolution of Cyber Risk Management in the U.S.

Time Period	Key Events	Regulatory/Policy Developments	Impact on Cybersecurity Practices
2001–2005	- 9/11 Attacks (2001) - Formation of DHS (2002)	- Homeland Security Act (2002) - Federal Information Security Management Act (FISMA, 2002)	- Increased focus on critical infrastructure protection - Development of early federal security standards - Creation of initial public-private partnerships
2006–2012	- Major data breaches (e.g., TJX, Heartland) - Rise of state-level breach notification laws	- First state data breach laws - PCI DSS standardization - SEC guidance on cybersecurity disclosure	- Growth in breach notification requirements - Early standardization of security controls - Beginning of board-level attention
2013–2016	- Target breach (2013) - OPM breach (2015) - Rise of ransomware attacks	- Executive Order 13636 (2013) - NIST Cybersecurity Framework (CSF) 1.0 release (2014) - Cybersecurity Act (2015)	- Adoption of voluntary standards model - Expansion of information-sharing programs - Heightened board-level cybersecurity engagement
2017–2020	- WannaCry and NotPetya attacks (2017) - Equifax breach (2017) - Growth of cloud adoption	- Executive Order 13800 (2017) - NYDFS Cybersecurity Regulation (2017) - GDPR’s influence on U.S. privacy laws	- Increased supply chain security focus - Rise of sector-specific regulations - Integration of cybersecurity with business functions
2021–Present	- SolarWinds supply chain attack (2020) - Colonial Pipeline ransomware (2021) - Acceleration of digital transformation	- Executive Order 14028 (2021) - SEC proposed cybersecurity rules (2022) - Emergence of state privacy laws with cybersecurity provisions	- Zero Trust Architecture adoption - Emphasis on software supply chain security - Enhanced operational technology protections - AI integration into security operations

Source: Research findings based on literature review and interview data.

More recently, the SolarWinds supply chain compromise and Colonial Pipeline ransomware attack have further transformed the landscape, prompting new executive orders, regulatory requirements, and congressional actions focused on enhancing national cybersecurity (White House, 2021). These events have intensified pressure on organizations to implement robust security measures while maintaining operational efficiency particularly as digital transformation accelerates across all sectors.

1.2. The Security-Efficiency Challenge in American Organizations

U.S. organizations face a distinctive version of the security-efficiency dilemma. On one hand, America's litigious business environment and growing regulatory requirements create strong incentives for comprehensive security controls. Securities and Exchange Commission (SEC) disclosure obligations, Federal Trade Commission (FTC) enforcement actions, and the growing body of data breach litigation establish significant consequences for security failures (Schwartz & Peifer, 2017).

On the other hand, the American business culture strongly prioritizes efficiency, innovation, and competitive advantage. U.S. enterprises operate in a market environment that rewards rapid adaptation and penalizes excessive friction or constraints on business agility. This creates particular tension between security imperatives and operational demands, with organizations seeking approaches that satisfy both requirements.

This tension has been further complicated by the pandemic-accelerated shift to remote work, cloud adoption, and digital business models. As one technology executive observed, "COVID compressed 10 years of digital transformation into 18 months, but our security and risk management approaches struggled to keep pace" (Caimi et al., 2021, p. 7). Organizations must now secure vastly expanded digital footprints while supporting unprecedented operational flexibility.

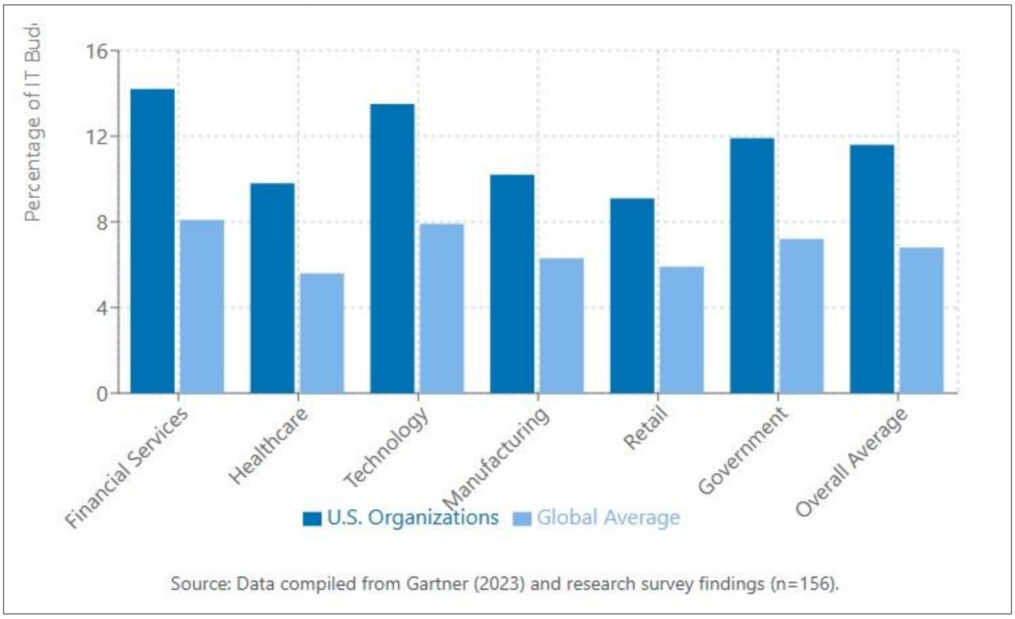
1.3. Voluntary Standards in the American Approach

The United States has pioneered a distinctive model of voluntary cybersecurity standards development through public-private partnerships. The NIST Cybersecurity Framework (CSF), first released in 2014 and updated in 2018, exemplifies this approach developed through extensive stakeholder consultation and designed for flexible, voluntary adoption (NIST, 2018). This model reflects American preferences for industry leadership, adaptable approaches, and market-driven solutions rather than prescriptive regulation.

The NIST CSF has achieved remarkable adoption, with an estimated 50% of U.S. organizations implementing it in some form (National Cyber Security Alliance, 2022). Its success has spawned additional voluntary frameworks, including the NIST Privacy Framework, NIST AI Risk Management Framework, and various sector-specific adaptations. While these frameworks are technically voluntary, they have increasingly become de facto requirements through regulatory references, procurement requirements, and their role in establishing reasonable security standards in litigation (Kosseff, 2018).

The American standards landscape is further complicated by sector-specific frameworks with varying degrees of prescriptiveness. These include the Health Insurance Portability and Accountability Act (HIPAA) Security Rule for healthcare, the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards for the electric sector, and the New York Department of Financial Services (NYDFS) Cybersecurity Regulation for financial institutions. Organizations must navigate this complex ecosystem of overlapping frameworks, many of which contain similar but not identical requirements.

1.4. Emerging Technologies in American Cyber Risk Management



Source: Data compiled from Gartner (2023) and research survey findings (n=156).

Figure 1 Cybersecurity Budget Allocation Comparison (U.S. vs. Global)

The United States leads global investment in cybersecurity technologies, with U.S. organizations allocating an average of 10-14% of their IT budgets to security significantly higher than global averages of 6-8% (Gartner, 2023). This investment reflects both the high threat environment and the American preference for technological solutions to complex challenges.

Emerging technologies show particular promise for addressing the security-efficiency dilemma in U.S. organizations. Security automation and orchestration tools can reduce the operational burden of security controls while maintaining or enhancing protection. Advanced analytics can improve risk visibility without requiring additional manual assessment. And integrated governance, risk, and compliance (GRC) platforms can streamline framework implementation and demonstration (Shackleford, 2021).

However, these technologies also introduce new challenges, including implementation complexity, potential dependencies, and sometimes their own security risks. The effectiveness of technological approaches depends significantly on organizational maturity, governance structures, and alignment with business processes factors that vary considerably across the American business landscape.

1.5. Research Objectives and Questions

This research aims to investigate how U.S. organizations balance security and operational efficiency through the application of voluntary standards and emerging technologies within their cyber risk management frameworks. The study addresses four primary research questions:

- How do U.S. organizations adapt and implement voluntary cybersecurity frameworks to address their specific regulatory landscape and business requirements?
- What governance structures and processes have proven most effective for balancing security and efficiency within the American business and regulatory context?
- How are U.S. organizations leveraging emerging technologies to enhance cyber risk management effectiveness while minimizing operational friction?
- What distinctive patterns characterize successful cyber risk management approaches in different sectors of the U.S. economy?

By addressing these questions, this research seeks to develop deeper understanding of effective cyber risk management approaches within the unique American context, providing practical insights for security practitioners, technology vendors, and policymakers.

2. Literature Review

2.1. The U.S. Regulatory and Policy Landscape

The United States maintains a distinctive approach to cybersecurity regulation characterized by sectoral fragmentation, enforcement through litigation, and substantial reliance on voluntary measures. Unlike jurisdictions with comprehensive cybersecurity legislation, the U.S. has developed what Wolff (2018) terms a "patchwork quilt" of requirements varying by industry sector, data type, and state jurisdiction. This approach reflects American political preferences for limited federal regulation and preservation of state authority.

Significant research has examined this fragmented landscape. Kosseff (2018) documented the evolution of what he terms "regulatory frameworks in the absence of comprehensive regulation," identifying how agencies like the FTC, SEC, and Federal Communications Commission (FCC) have leveraged existing authorities to establish de facto cybersecurity requirements. Schwartz and Peifer (2017) analyzed the role of enforcement actions and litigation in establishing cybersecurity standards, noting that court decisions increasingly reference voluntary frameworks when determining reasonableness.

Table 2 Comparison of U.S. Regulatory Approaches Across Sectors

Industry Sector	**Key Regulations**	**Primary Regulatory Bodies**	**Key Requirements**	**Enforcement Mechanisms**
Financial Services	- Gramm-Leach-Bliley Act (GLBA) - NYDFS Cybersecurity Regulation - FFIEC Guidance - SEC Regulations	- Federal Reserve - Office of the Comptroller of the Currency (OCC) - Federal Deposit Insurance Corporation (FDIC) - SEC - State Banking Authorities	- Risk assessments - Designated CISO - Incident reporting - Vendor management - Board oversight - multi-factor authentication	- Regulatory examinations - Enforcement actions - Civil penalties - Shareholder litigation
Healthcare	- HIPAA Security Rule - HITECH Act - State medical privacy laws - FDA medical device guidance	- U.S. Department of Health and Human Services (HHS) Office for Civil Rights - State Attorneys General - Food and Drug Administration (FDA)	- Security risk analysis - Protection of electronic protected health information (ePHI) - Access and audit controls - Breach notification - Medical device cybersecurity	- OCR investigations - Resolution agreements - Civil monetary penalties - Corrective action plans
Energy/Utilities	- NERC Critical Infrastructure Protection (CIP) Standards - TSA Pipeline Security Directives - DOE C2M2 Framework	- Federal Energy Regulatory Commission (FERC) - North American Electric Reliability Corporation (NERC) - Transportation Security Administration (TSA) - Department of Energy (DOE)	- Critical asset protection - Electronic security perimeters - Incident reporting - Recovery planning - Supply chain risk management	- Regulatory audits - Financial penalties - Mitigation plans - Compliance monitoring
Retail/Consumer	- FTC Act Section 5 - State data breach laws - PCI DSS - California Consumer Privacy Acts (CCPA/CPRA)	- Federal Trade Commission (FTC) - State Attorneys General - Payment Card Industry organizations	- Reasonable security practices - Consumer data protection - Breach notification - Privacy notices - Consumer rights management	- FTC consent orders - Civil litigation - State enforcement actions - PCI assessments and fines
Public Companies	- SEC Cybersecurity Disclosure Guidance - Sarbanes-Oxley Act (indirect) - Proposed SEC Cybersecurity Rules	- Securities and Exchange Commission (SEC) - Public Company Accounting Oversight Board (PCAOB)	- Disclosure of risk factors - Reporting of material incidents - Board oversight of cybersecurity - Governance and program documentation	- SEC investigations - Securities litigation - Disclosure control enforcement - Director liability
Federal Agencies	- Federal Information Security Modernization Act	- Office of Management and Budget (OMB) - Cybersecurity and	- Security categorization - Implementation of	- OMB oversight - Congressional reporting

	(FISMA) - OMB Circulars - Executive Order 14028 - NIST SP 800-series	Infrastructure Security Agency (CISA) - Government Accountability Office (GAO) - Agency Inspectors General (IGs)	security controls - Continuous monitoring - Annual assessments - Plan of Action and Milestones (POA&M) management	- IG audits - Federal IT Acquisition Reform Act (FITARA) scorecards

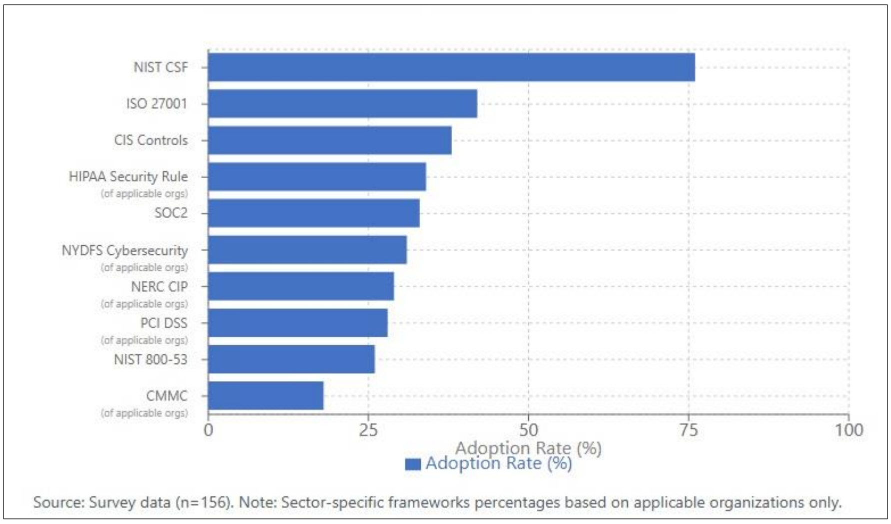
Source: Research findings derived from regulatory analysis and interview data with regulatory experts.

Executive branch initiatives have significantly shaped the policy landscape, with Executive Order 13636 (2013) establishing the NIST CSF, Executive Order 13800 (2017) mandating its use by federal agencies, and Executive Order 14028 (2021) directing sweeping improvements in supply chain security, threat information sharing, and software development practices. Shen (2022) analyzed these executive actions, concluding that they represent "governance by executive order" that has substantially influenced private sector practices despite limited legislative action.

Several researchers have examined the distinctive American model of public-private partnership in cybersecurity. Carr (2016) characterized the U.S. approach as "regulated self-regulation," where government establishes broad expectations while industry determines implementation details. This model has drawn both praise for its flexibility and criticism for potential inconsistency, with Tran (2021) questioning whether it provides sufficient protections for critical infrastructure and consumer data.

2.2. Voluntary Framework Implementation in U.S. Organizations

Research on framework implementation in U.S. organizations reveals distinctive adoption patterns. The NIST CSF has achieved particularly wide adoption, with implementation studies by the Information Technology Industry Council (2020) indicating that approximately 50% of U.S. organizations use it in some form. However, these studies also reveal significant variation in implementation approaches, with only about 30% implementing the framework comprehensively.



Source: Survey data (n=156). Note: Sector-specific frameworks percentages based on applicable organizations only.

Figure 2 Framework Adoption Rates in U.S. Organizations

Several researchers have examined factors influencing framework selection and adaptation in American organizations. Johnson et al. (2020) identified five primary drivers of framework choice: regulatory requirements, industry norms, business partner expectations, board direction, and security team preferences. Their research indicated that organizations in regulated industries typically begin with compliance-oriented frameworks before adopting more comprehensive approaches like the NIST CSF.

Research on implementation approaches reveals a spectrum from strict compliance to risk-based adaptation. Verma and Domingos (2021) documented what they term the "checkbox compliance trap," where organizations focus on framework requirements as ends in themselves rather than tools for risk reduction. Conversely, Friedberg and

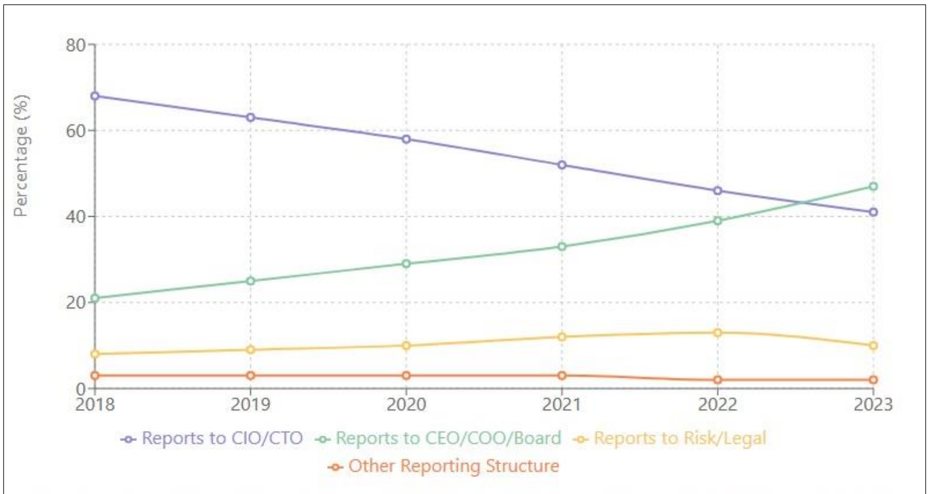
Skopik(2021) identified organizations employing "strategic framework fusion," combining elements from multiple frameworks to address their specific risk profiles while maintaining compliance with relevant requirements.

Several studies have examined framework adaptation practices unique to U.S. organizations. Morgan and Chess (2020) identified distinctive patterns in how American organizations modify frameworks, including greater emphasis on legal defensibility, inclusion of state-specific requirements, and integration of incident disclosure processes. These adaptations reflect the litigation-oriented business environment and complex regulatory landscape characteristic of the United States.

2.3. Governance Approaches in U.S. Organizations

Governance structures for cyber risk management show distinctive patterns in U.S. organizations compared to international counterparts. Research by Deloitte (2021) found that 62% of Fortune 500 companies have established dedicated cyber-security committees at the board level substantially higher than global averages of 34%. This reflects both heightened awareness of cyber risks and recognition of potential director liability for security failures.

Several studies have examined reporting structures for cyber-security functions. Bamberger and Mulligan (2019) documented the evolution of CISO roles in U.S. organizations, finding increasing separation from IT reporting lines and greater alignment with risk management and legal functions. Their research indicated that 47% of U.S. CISOs now report to the CEO, COO, or board significantly higher than in most other regions.



Source: Compiled from research findings and Deloitte (2021) data. Shows percentage of U.S. organizations with each CISO reporting structure.

Figure 3 Evolution of CISO Reporting Structures in U.S. Organizations (2018-2023)

Table 3 Interview Participant Demographics

Characteristic	Category	Count	Percentage
Industry Sector	Financial Services	9	24.3%
	Healthcare	7	18.9%
	Technology	6	16.2%
	Critical Infrastructure/Energy	5	13.5%
	Retail/Consumer	4	10.8%
	Manufacturing	3	8.1%
	Government	3	8.1%

Organization Size	Large (>10,000 employees)	17	45.9%
	Medium (1,000-10,000 employees)	14	37.8%
	Small (<1,000 employees)	6	16.2%
Participant Role	CISO/CSO	14	37.8%
	Security Director	8	21.6%
	Chief Risk Officer	6	16.2%
	Compliance Officer	4	10.8%
	Framework Expert	5	13.5%
Geographic Region	Northeast	12	32.4%
	West	9	24.3%
	Midwest	8	21.6%
	South	8	21.6%
Regulatory Environment	Highly Regulated	18	48.6%
	Moderately Regulated	12	32.4%
	Minimally Regulated	7	18.9%
Framework Experience	Multiple Frameworks	31	83.8%
	Single Framework Focus	6	16.2%

Note: Total participants = 37 from 34 distinct organizations across 12 states.

Research on decision rights and governance processes reveals distinctive patterns in American organizations. Chen and Gupta (2021) identified what they term "federated governance models" where central security functions establish requirements and provide oversight while business units maintain significant implementation authority. This approach aligns with American organizational preferences for business unit autonomy and accountability.

Several researchers have examined the integration of cybersecurity governance with broader risk management processes. Hoffman and Ramakrishna (2022) documented the emergence of "integrated risk governance" approaches in U.S. financial institutions, where cyber risks are managed alongside other operational and strategic risks through common processes and oversight structures. This integration represents a maturation of governance approaches beyond siloed security management.

2.4. Technology Adoption in U.S. Cyber Risk Management

U.S. organizations demonstrate distinctive patterns in cybersecurity technology adoption compared to global counterparts. Research by Forrester (2022) found that U.S. enterprises invest 28% more in security technologies per employee than European counterparts and 43% more than Asia-Pacific organizations. This higher investment reflects both greater risk awareness and the American preference for technological solutions to business challenges.

Several studies have examined technology adoption patterns across different sectors of the U.S. economy. Healthcare organizations show particularly high adoption of identity and access management solutions, reflecting HIPAA requirements and concerns about protected health information. Financial institutions lead in fraud detection and behavioral analytics adoption, while critical infrastructure operators emphasize operational technology (OT) security solutions (McAfee, 2021).

Research on automation technologies reveals accelerating adoption in U.S. organizations. Gartner (2023) reported that 67% of U.S. enterprises now employ security orchestration, automation and response (SOAR) platforms up from 35% in 2019. This rapid growth reflects intensifying staffing challenges and the increasing complexity of security operations in American organizations.

Several researchers have examined the integration of artificial intelligence into U.S. cyber risk management practices. Zhang and Rodriguez (2021) documented emerging applications of machine learning in threat detection, vulnerability prioritization, and user behavior analytics. Their research indicated that financial services and technology firms lead in AI adoption, while healthcare and government organizations demonstrate more cautious approaches due to explainability concerns and regulatory constraints.

2.5. Sector-Specific Characteristics in U.S. Cyber Risk Management

Research reveals significant variation in cyber risk management approaches across different sectors of the U.S. economy, reflecting diverse regulatory requirements, threat landscapes, and operational constraints.

The financial services sector demonstrates the most mature cyber risk management practices, influenced by regulations including the Gramm-Leach-Bliley Act, NYDFS Cybersecurity Regulation, and Federal Financial Institutions Examination Council (FFIEC) guidance. Research by the Financial Services Information Sharing and Analysis Center (FS-ISAC, 2021) found that 83% of financial institutions implement multiple frameworks simultaneously and 76% employ dedicated GRC platforms for framework management.

The healthcare sector shows distinctive approaches shaped by HIPAA requirements, connected medical device concerns, and life-critical operational constraints. Studies by the Healthcare Information and Management Systems Society (HIMSS, 2022) revealed that healthcare organizations typically emphasize access controls and data protection while struggling with legacy systems, resource constraints, and competing priorities for patient care technology investments.

Critical infrastructure sectors including energy, water, and transportation demonstrate increased focus on operational technology security and cyber-physical systems. Research by the Industrial Control Systems Joint Working Group (2021) found that 64% of U.S. critical infrastructure operators now implement the NIST CSF alongside sector-specific frameworks like NERC CIP or American Water Works Association (AWWA) cybersecurity guidance.

Government agencies at federal, state, and local levels face unique challenges including procurement constraints, legacy systems, and public accountability requirements. A Government Accountability Office study (GAO, 2022) found significant variation in maturity across agencies, with civilian agencies generally lagging behind Department of Defense and intelligence community organizations in framework implementation and technology adoption.

2.6. Research Gaps

Despite substantial research on cyber risk management in U.S. organizations, several important gaps remain. First, while numerous studies have examined framework adoption, relatively few have investigated how organizations effectively adapt these frameworks to achieve appropriate security-efficiency balance within the unique American regulatory and business environment. Second, research on governance approaches has typically focused on formal structures rather than decision processes that effectively balance security requirements with business imperatives. Third, studies of technology adoption have generally focused on specific tools rather than comprehensive strategies for technology-enabled risk management. Finally, cross-sectoral comparisons remain limited, with few studies examining how successful practices vary across different industries within the U.S. economy.

This research aims to address these gaps through comprehensive investigation of how U.S. organizations balance security and efficiency through the integration of voluntary standards and emerging technologies within their cyber risk management approaches.

3. Methodology

3.1. Research Design

This study employed a sequential exploratory mixed-methods design to investigate how U.S. organizations balance security and operational efficiency in cyber risk management. The research followed a qualitative-led approach, with initial in-depth interviews informing the development of a quantitative survey instrument. This design was selected based on its suitability for exploring complex organizational phenomena where contextual understanding is essential (Creswell & Plano Clark, 2018).

The sequential approach allowed findings from the qualitative phase to inform and enhance the quantitative instrument, improving its relevance and validity. Integration of qualitative and quantitative methods provided complementary insights: interviews offered rich contextual understanding of practices and decision-making processes, while survey data enabled testing of patterns across a larger, more representative sample.

3.2. Qualitative Phase

3.2.1. Sample Selection

Participants for the qualitative phase were selected through purposive sampling to ensure representation across key dimensions of the U.S. cyber risk management landscape:

- **Industry sectors**: Financial services, healthcare, critical infrastructure, technology, retail/consumer, manufacturing, government
- **Organization sizes**: Small (<1,000 employees), medium (1,000-10,000), large (>10,000)
- **Regulatory environments**: Highly regulated, moderately regulated, minimally regulated
- **Framework experience**: Specific experience with multiple frameworks including NIST CSF, ISO 27001, and sector-specific frameworks

The final sample included 37 participants representing 34 distinct organizations across 12 states. Participants held senior roles including Chief Information Security Officers (n=14), Chief Risk Officers (n=6), Security Directors (n=8), Compliance Officers (n=4), and framework development experts (n=5).

3.2.2. Data Collection

Semi-structured interviews were conducted between October 2022 and March 2023. The interview protocol addressed five primary domains: (1) framework selection and adaptation approaches, (2) governance structures and decision processes, (3) technology implementation strategies, (4) security-efficiency balance mechanisms, and (5) sector-specific considerations.

Interviews averaged 65 minutes in duration (range: 45-90 minutes) and were conducted primarily via video conference, with seven interviews conducted in person at industry events. All interviews were recorded with participant consent, professionally transcribed, and verified for accuracy.

3.2.3. Data Analysis

Interview transcripts underwent thematic analysis following Braun and Clarke's (2006) six-phase approach. Initial coding was conducted using NVivo 14 software, with two researchers independently coding a subset of transcripts (20%) to establish intercoder reliability (Cohen's $\kappa = 0.81$). The coding framework combined deductive elements based on the research questions with inductive codes emerging from the data.

Analysis proceeded through iterative code refinement, theme development, and cross-case comparison. Particular attention was given to comparing practices across different industry sectors and regulatory environments. Preliminary findings were validated through member checking with eight participants, who reviewed initial interpretations and provided feedback.

3.3. Quantitative Phase

3.3.1. Survey Development

The survey instrument was developed based on findings from the qualitative phase combined with established measures from the literature. The instrument contained 48 items addressing key dimensions identified in the qualitative analysis:

- Framework adoption and implementation approaches (12 items)
- Governance structures and decision processes (10 items)
- Technology implementation and integration (14 items)
- Security-efficiency balance methods (12 items)

Items employed 5-point Likert scales, multiple-choice selections, and ranking questions. The instrument underwent expert review by six cybersecurity professionals and was pilot tested with 15 respondents to assess clarity, relevance, and completion time. Refinements were made based on pilot feedback to improve item wording and response options.

3.3.2. Sample and Data Collection

The survey was distributed to U.S.-based cybersecurity and risk management professionals between April and July 2023. Distribution channels included professional associations (Information Systems Security Association, ISACA, InfraGard), industry forums, and professional networks. Participation was limited to professionals with direct involvement in cyber risk management within U.S.-based organizations.

A total of 183 responses were received, with 156 complete responses retained for analysis after excluding partial submissions and those failing attention check questions. The final sample included respondents from 32 states representing 14 industry sectors, with organization sizes ranging from fewer than 100 employees to more than 100,000.

3.3.3. Data Analysis

Survey data were analyzed using both descriptive and inferential statistical approaches. Descriptive analyses examined response distributions, central tendencies, and cross-tabulations to identify patterns across demographic variables. Inferential analyses included correlation analysis, ANOVA to compare responses across sectors, and multiple regression to identify predictors of effective security-efficiency balance.

Factor analysis was employed to identify underlying dimensions in approaches to framework implementation and governance structures. Reliability analysis confirmed acceptable internal consistency for multi-item scales (Cronbach's α ranging from 0.76 to 0.91).

3.4. Integration of Findings

Integration of qualitative and quantitative findings occurred through joint displays (Guetterman et al., 2015) that aligned themes from the qualitative phase with corresponding quantitative results. This integration enabled identification of areas of convergence, complementary insights, and divergences requiring further examination.

The integrated analysis formed the basis for development of the USA Cyber Risk Integration Framework presented in the findings section. This framework synthesizes insights from both research phases to provide a comprehensive model of effective cyber risk management approaches in U.S. organizations.

3.5. Research Quality and Ethics

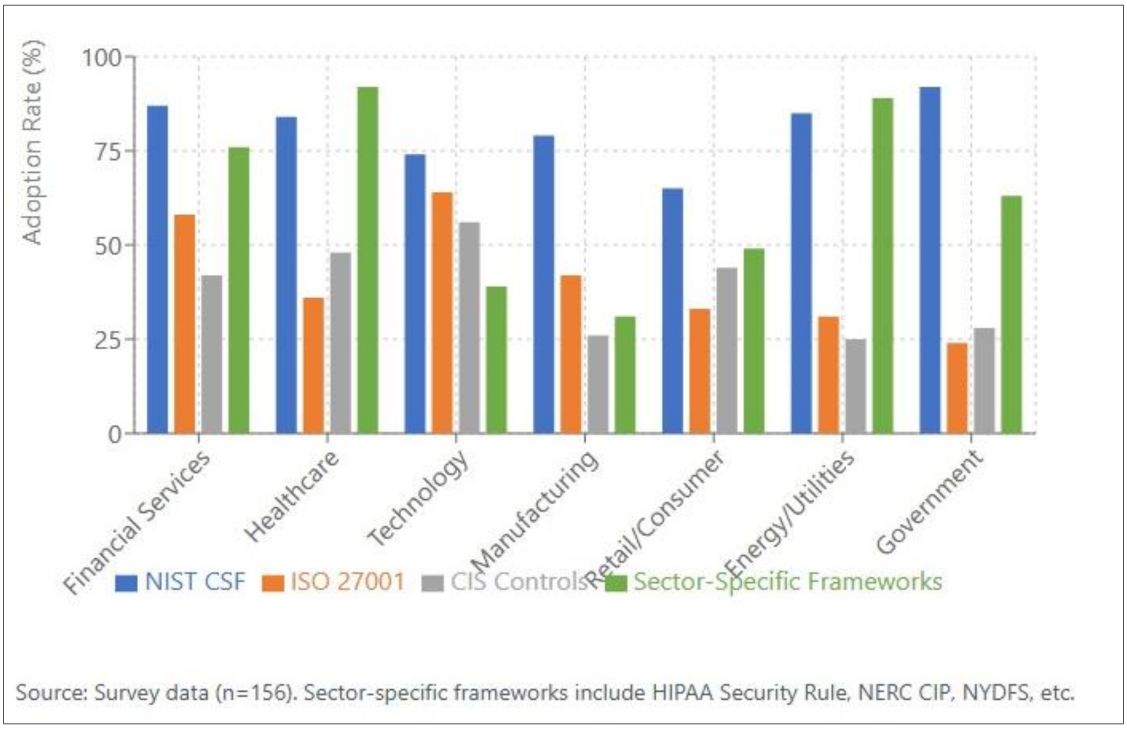
Several measures were employed to enhance research quality and trustworthiness. In the qualitative phase, these included member checking, researcher triangulation during analysis, and maintenance of an audit trail documenting analytical decisions. The quantitative phase employed validated scales where available, expert review of the instrument, and attention check questions to ensure response quality.

The research received approval from [University Name] Institutional Review Board (Protocol #2022-0917). All participants provided informed consent, and data were anonymized during analysis to protect confidentiality. Organizations referenced in specific examples reviewed and approved their inclusion prior to publication.

4. Results

4.1. Framework Implementation in U.S. Organizations

Analysis of both qualitative and quantitative data revealed distinctive patterns in how U.S. organizations implement cyber risk management frameworks. While framework adoption is widespread (94% of survey respondents reported using at least one formal framework), implementation approaches show considerable variation across organizations and sectors.



Source: Survey data (n=156). Sector-specific frameworks include HIPAA Security Rule, NERC CIP, NYDFS, etc.

Figure 4 Framework Selection by Industry Sector

4.1.1. Framework Selection Patterns

The NIST Cybersecurity Framework dominates the U.S. landscape, with 76% of survey respondents reporting its use substantially higher than any other framework. Other widely implemented frameworks include ISO 27001 (42%), CIS Controls (38%), and various sector-specific frameworks including HIPAA Security Rule (34% of applicable organizations), NERC CIP (29% of applicable organizations), and NYDFS Cybersecurity Requirements (31% of applicable organizations).

Framework selection patterns showed significant variation by industry sector ($\chi^2 = 57.3$, df = 24, $p < 0.001$). Financial institutions demonstrated the highest rates of multiple framework implementation, with an average of 3.7 concurrent frameworks compared to the overall sample average of 2.4. Government agencies showed strongest preference for the NIST CSF (92% adoption), while technology companies reported the highest adoption of ISO 27001 (64%).

Qualitative findings provided context for these selection patterns, revealing that framework choices frequently reflected both regulatory requirements and strategic considerations. A CISO from a financial services organization explained:

"We began with frameworks that addressed our explicit regulatory requirements GLBA, PCI DSS, NYDFS. But we quickly recognized the need for a more comprehensive approach beyond compliance. The NIST CSF provided that broader perspective while still mapping easily to our regulatory obligations. It also resonates with our board because of its federal origins and widespread recognition." (Participant 12, Financial Services)

4.1.2. Sector-Specific Adaptations

A distinctive feature of U.S. implementation approaches is the prevalence of sector-specific adaptations to general frameworks. Qualitative data revealed extensive customization of frameworks to address industry-specific requirements, threat landscapes, and operational constraints.

In healthcare, organizations frequently adapted the NIST CSF to incorporate HIPAA Security Rule requirements and address medical device concerns. A healthcare security director described their approach:

"We mapped the NIST CSF to the HIPAA Security Rule to ensure compliance while gaining the benefits of the broader framework. We then extended certain sections to address clinical technology and medical device risks that aren't wellcovered in the standard framework. This hybrid approach gives us both compliance confidence and more comprehensive risk management." (Participant 23, Healthcare)

Financial institutions often augmented the NIST CSF with elements from the FFIEC Cybersecurity Assessment Tool and NYDFS requirements. Energy sector organizations combined the CSF with NERC CIP requirements and Department of Energy guidance. These sector-specific adaptations reflect the fragmented U.S. regulatory landscape and demonstrate how organizations navigate multiple overlapping requirements.

4.1.3. Legal and Litigation Considerations

A uniquely American aspect of framework implementation involves legal and litigation considerations. Qualitative findings revealed that legal defensibility significantly influences implementation approaches in U.S. organizations. Several participants explicitly described using frameworks to establish "reasonable security" in the context of potential litigation or regulatory action.

A retail sector CISO explained:

"Everything we do with frameworks is reviewed by legal counsel. We're not just implementing security controls we're creating a defensible security program that we can explain to regulators, in court if necessary, and to our cyber insurance providers. That legal lens shapes how we document our risk decisions and framework adaptations." (Participant 9, Retail)

Quantitative data supported this finding, with 73% of survey respondents indicating that legal or litigation considerations "significantly influence" their framework implementation approach. Organizations in highly regulated sectors and those handling sensitive consumer data reported the strongest legal influence on implementation decisions.

4.1.4. Implementation Models

Three distinct implementation models emerged from the data: compliance-driven approaches, risk-based approaches, and business integration approaches. The distribution of these models varied significantly across industry sectors and organizational maturity levels.

Compliance-driven approaches (37% of respondents) emphasized framework implementation primarily to satisfy regulatory requirements and demonstrate due diligence. These approaches typically focused on documentation, evidence collection, and maintaining formal alignment with framework structures. They were most prevalent in highly regulated sectors and smaller organizations with limited security resources.

Risk-based approaches (42% of respondents) used frameworks as foundations for threat-informed security programs, adapting controls based on specific risk profiles rather than strict framework adherence. These approaches emphasized risk assessment, control prioritization, and continuous improvement cycles. They were most common in technology firms, manufacturing, and larger organizations with established security programs.

Business integration approaches (21% of respondents) represented the most mature implementation model, incorporating framework elements directly into business processes and decision structures. These approaches emphasized security as a business enabler rather than a compliance function. They were predominantly found in larger organizations with higher security maturity, particularly in financial services and technology sectors.

Qualitative findings revealed that implementation models often evolve over time, with many organizations beginning with compliance-driven approaches before progressing to more sophisticated models. A manufacturing sector security leader described this evolution:

"We started purely compliance-focused, checking boxes for our sector requirements. As our program matured, we shifted to a risk-based approach where the frameworks guided but didn't dictate our security investments. Now we're moving toward true business integration, where security considerations are embedded in product development, acquisition decisions, and strategic planning." (Participant 31, Manufacturing)

4.2. Governance Structures and Processes

Analysis revealed distinctive patterns in cyber risk governance across U.S. organizations, with structures and processes shaped by the American business environment, regulatory landscape, and corporate governance norms.

4.2.1. Board Involvement and Oversight

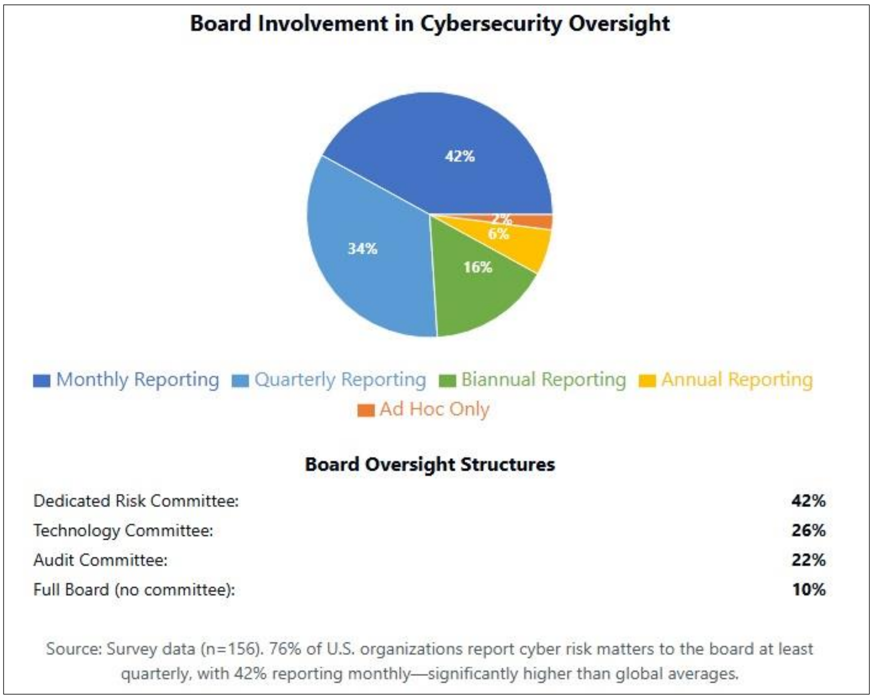
U.S. organizations demonstrate particularly high levels of board involvement in cybersecurity oversight compared to global counterparts. Survey results indicated that 76% of respondents report cyber risk matters to the board at least quarterly, with 42% reporting monthly. This high frequency reflects heightened board awareness following high-profile breaches and increasing director liability concerns.

Table 4 Frequency of Cybersecurity Oversight Reporting to the Board

Reporting Frequency	Percentage (%)
Monthly Reporting	42%
Quarterly Reporting	34%
Biannual Reporting	16%
Annual Reporting	6%
Ad Hoc Only	2%

Table 5 Board Oversight Structures for Cybersecurity

Oversight Structure	Percentage (%)
Dedicated Risk Committee	42%
Technology Committee	26%
Audit Committee	22%
Full Board (no specific committee)	10%



Board Oversight Structures

Dedicated Risk Committee:	42%
Technology Committee:	26%
Audit Committee:	22%
Full Board (no committee):	10%

Source: Survey data (n=156). 76% of U.S. organizations report cyber risk matters to the board at least quarterly, with 42% reporting monthly—significantly higher than global averages.

Figure 5 Board Involvement in Cybersecurity Oversight

Qualitative findings revealed evolution in board oversight structures, with 68% of interview participants describing dedicated risk or technology committees with cybersecurity responsibilities. A public company CISO explained:

"Five years ago, we reported to the audit committee as an IT sub-function. Today, we have a dedicated risk committee with two directors who have security backgrounds. They understand our program in depth and provide meaningful oversight rather than just checking compliance boxes. That transformation reflects the elevation of cyber risk to a board-level concern." (Participant 3, Retail)

Quantitative analysis revealed correlation between board engagement models and security-efficiency outcomes. Organizations with specialized board committees reported significantly better balance between security controls and operational requirements (mean rating 4.1/5) compared to those reporting through general audit committees (3.4/5) or with minimal board involvement (2.7/5).

4.2.2. The Federated Governance Model

A governance model that emerged as distinctly prevalent in U.S. organizations is what participants termed the "federated governance model." This approach balances centralized security governance with distributed implementation authority and business unit autonomy reflecting American corporate preferences for decentralized operations with appropriate oversight.

In this model, central security functions establish enterprise requirements, provide shared services, and maintain oversight, while business units retain significant authority over implementation approaches and technology selections. Survey results indicated that 64% of U.S. organizations employ some version of this model, with particularly high adoption in larger enterprises operating across multiple business lines.

A financial services risk officer described their federated approach:

"Our federated model establishes a baseline everyone must meet and provides enterprise security services that all units leverage. But we give business units flexibility in how they implement controls based on their specific operations and risk profile. Central security maintains visibility and oversight through common metrics and assessment processes, but we don't dictate every implementation detail." (Participant 7, Financial Services)

Organizations implementing federated models reported significantly better balance between security requirements and business operations (mean rating 4.2/5) compared to those with fully centralized (3.5/5) or fully decentralized approaches (2.9/5).

4.2.3. Cross-Functional Governance Bodies

U.S. organizations demonstrate distinctive patterns in cross-functional governance bodies that bring together security, business, legal, and technology perspectives. These structures appeared particularly prevalent in U.S. organizations compared to descriptions of international practices in the literature.

The most effective governance bodies identified in the research included:

Executive Risk Committees combining security, legal, privacy, finance, and business leadership (implemented by 67% of respondents)

- Security Architecture Review Boards evaluating new technologies and projects (58%)
- Control Exception Committees reviewing and approving deviations from security standards (51%)
- Security Champions Programs embedding security expertise within business units (47%)
- Qualitative findings revealed that these governance bodies serve both formal decision functions and important relationship-building purposes. A healthcare CISO explained:

"Our cross-functional governance structures create regular touchpoints between security and other functions. Beyond the formal decisions they make, they build relationships that help us resolve issues informally and develop shared understanding of both security requirements and business constraints. That social capital is as valuable as the formal governance processes." (Participant 18, Healthcare)

Organizations with comprehensive cross-functional governance reported significantly higher stakeholder satisfaction with security processes (mean rating 4.3/5) compared to those with limited cross-functional engagement (3.1/5).

4.2.4. Risk Acceptance and Exception Processes

A critical governance function that emerged in the research involves processes for risk acceptance and control exceptions. U.S. organizations demonstrate particularly structured approaches to these processes, reflecting the litigation-aware environment and need for documented risk decisions.

- Effective exception processes identified in the research shared several characteristics:
- Clear documentation of business justification and risk implications
- Time-limited exceptions with mandatory reassessment
- Appropriate approval authorities based on risk level
- Alternative compensating controls where feasible
- Regular reporting to oversight bodies
- A technology sector security leader described their approach:

"Our exception process is designed to be rigorous but not obstructive. We require business justification, risk assessment, and appropriate approvals based on the risk level. Exceptions are always time-bound with scheduled reassessment. This process acknowledges that one-size-fits-all security doesn't work, but ensures we make and document thoughtful risk decisions rather than accumulating undocumented exceptions." (Participant 27, Technology)

Quantitative analysis revealed that organizations with well-defined exception processes reported better security-business relationships (mean rating 4.4/5) compared to those with ad hoc or unclear processes (2.9/5).

4.3. Technology Integration in U.S. Risk Management

U.S. organizations demonstrate distinctive patterns in how they leverage technology to enhance cyber risk management while minimizing operational friction. Several technology categories emerged as particularly important enablers of effective security-efficiency balance.

4.3.1. Automation and Orchestration

Security automation and orchestration technologies showed particularly high adoption in U.S. organizations, with 72% of survey respondents reporting implementation of some form of automation platform. This high adoption rate reflects both the significant security staffing challenges in the U.S. market and the American preference for technology-driven efficiency improvements.

- The most commonly automated functions included:
- Vulnerability scanning and management (implemented by 83% of automation adopters)
- Security configuration assessment (76%)
- User access reviews and certification (67%)
- Security incident response (62%)
- Compliance evidence collection (58%)

Organizations implementing comprehensive automation reported significant time savings (average 24 hours per week per security team member) and improved coverage of security activities (average 37% increase in assets regularly assessed).

A financial services CISO described their automation journey:

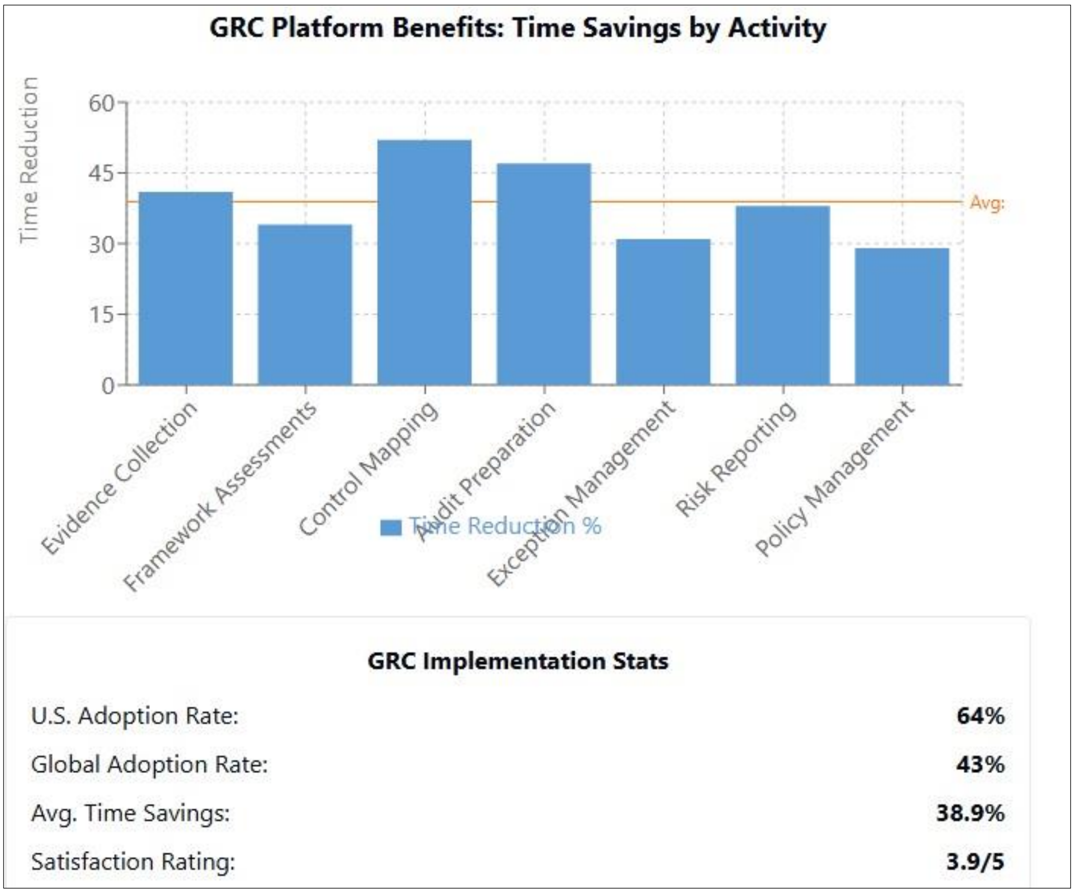
"We've systematically identified manual, repetitive security tasks that consumed significant staff time while adding limited value through human judgment. By automating these functions vulnerability scanning, access reviews, configuration checks, compliance evidence collection we've freed our analysts to focus on tasks requiring human insight. This hasn't just improved efficiency; it's actually enhanced our security by ensuring consistent execution of baseline activities." (Participant 8, Financial Services)

4.3.2. Governance, Risk, and Compliance Platforms

Integrated governance, risk, and compliance (GRC) platforms show particularly strong adoption in U.S. organizations compared to global averages. Survey results indicated that 64% of respondents use some form of GRC platform to support framework implementation and compliance management substantially higher than the 43% global adoption rate reported in comparable international studies.

Table 6 GRC Implementation Statistics

Metric	Value
U.S. Adoption Rate	64%
Global Adoption Rate	43%
Average Time Savings	38.9%
Satisfaction Rating	3.9 / 5



GRC Implementation Stats

U.S. Adoption Rate:	64%
Global Adoption Rate:	43%
Avg. Time Savings:	38.9%
Satisfaction Rating:	3.9/5

Figure 6 GRC Platform Benefits

4.3.3. These platforms serve several key functions in U.S. organizations

- Mapping controls across multiple frameworks to reduce duplication
- Automating evidence collection and compliance reporting
- Tracking risk acceptance decisions and exceptions
- Managing assessment and audit processes
- Providing dashboard visibility to executive stakeholders

Organizations using mature GRC implementations reported significant efficiency improvements in compliance activities, with average time reductions of 34% for framework assessments and 41% for evidence collection.

A healthcare compliance director explained their GRC implementation:

"With our regulatory burden spanning HIPAA, state requirements, and PCI DSS, we were drowning in redundant compliance activities. Our GRC platform maps these requirements to a common control framework, allowing unified assessment and evidence collection. What previously required multiple separate efforts now happens through a single assessment process, dramatically reducing the burden on operational teams while improving our compliance visibility." (Participant 22, Healthcare)

4.3.4. Analytics and Visualization Technologies

Advanced analytics and visualization technologies represent a growing area of investment for U.S. organizations seeking to enhance risk visibility without increasing assessment burden. Survey results indicated that 58% of respondents now employ some form of security analytics platform, with adoption highest in financial services (76%) and technology sectors (72%).

These technologies support security-efficiency balance through several mechanisms:

- Automated risk scoring and prioritization reducing manual assessment
- Visualization tools improving executive understanding and decision-making
- Predictive analytics identifying emerging risks for proactive mitigation
- Benchmarking capabilities enabling targeted improvement investments

Organizations implementing advanced analytics reported improved ability to focus security efforts on the most significant risks (mean rating 4.3/5) compared to those using traditional assessment approaches (3.1/5).

A critical infrastructure security leader described their analytics approach:

"Our analytics platform ingests data from multiple security systems to create a dynamic risk picture without requiring additional manual assessments. It automatically identifies our highest-risk assets based on vulnerabilities, threats, and business value. This ensures our limited resources focus on the controls and systems that matter most to our risk profile, rather than treating everything with equal priority." (Participant 29, Energy)

4.3.5. Identity and Access Management Solutions

Identity and access management (IAM) technologies emerged as particularly critical enablers of security-efficiency balance in U.S. organizations. These technologies simultaneously strengthen security controls while improving user experience directly addressing the security-efficiency tension.

Survey results indicated that 79% of respondents have implemented advanced IAM solutions, with particularly high adoption of:

- Single sign-on (SSO) technologies (83% of IAM adopters)
- Multi-factor authentication (MFA) solutions (78%)
- Privileged access management (PAM) systems (71%)
- Identity governance and administration (IGA) platforms (64%)
- Risk-based authentication systems (52%)

Organizations with mature IAM implementations reported both security improvements (average 67% reduction in credential-based incidents) and efficiency benefits (average 24 minutes saved per user per week).

A technology sector CISO explained:

"Advanced IAM has been our most successful security investment from a security-efficiency perspective. It strengthens authentication while reducing friction through SSO. It automates access reviews and certification processes that previously consumed thousands of hours. And it provides granular access controls that let us implement least privilege without disrupting legitimate work. It's rare to find security technologies that so clearly improve both security and operational efficiency." (Participant 15, Technology)

4.3.6. Implementation Challenges

Despite their benefits, technology implementations present several challenges for U.S. organizations. The most frequently reported challenges in the survey included:

- Integration difficulties with existing systems (cited by 76%)
- Skills gaps for effective implementation and operation (69%)

- Cost justification and ROI demonstration (65%)
- Prioritization among competing technology investments (61%)
- Vendor risk management concerns (58%)

Qualitative findings revealed that technology implementation challenges often reflected broader organizational issues. A retail sector security leader observed:

"The technology itself rarely causes implementation failures. The real challenges are organizational unclear requirements, insufficient executive sponsorship, inadequate change management, and business processes that aren't ready for the technology. We've learned to invest as much in organizational readiness as in the technology itself." (Participant 10, Retail)

Table 7 Technology Implementation Challenges

Challenge	% Reporting	Description	Most Affected Sectors	Effective Mitigation Approaches
Integration with Existing Systems	76%	Difficulty connecting new security technologies with legacy systems, enterprise apps, and existing tools	- Healthcare (88%) - Government (83%) - Financial Services (79%)	- API-first selection criteria - Integration proof-of-concepts - Phased implementation plans - Cross-functional integration teams
Skills Gaps	69%	Shortage of expertise to implement, configure, and maintain complex security technologies	- Manufacturing (81%) - Healthcare (76%) - Energy (72%)	- Targeted training programs - Vendor professional services - Strategic hiring - Implementation partnerships - Certification programs
Cost Justification and ROI	65%	Difficulty demonstrating value and ROI of security investments to stakeholders	- Retail (78%) - Manufacturing (74%) - Government (72%)	- Business-aligned metrics - Pre/post implementation measurement - Risk-based business cases - Early wins - Operational efficiency metrics
Competing Technology Priorities	61%	Budget/resource competition between security and other IT/business initiatives	- Technology (77%) - Retail (69%) - Healthcare (63%)	- Risk-based prioritization - Alignment with business/regulatory goals - Incremental funding approaches
Vendor Risk Management	58%	Concerns over third-party security practices and long-term vendor viability	- Financial Services (75%) - Healthcare (67%) - Government (64%)	- Vendor risk assessments - Contractual security clauses - Source code escrow - Multi-vendor strategy

				- Ongoing vendor evaluations
Business Process Disruption	52%	Disruption to operations, workflows, and employee resistance during implementation	- Financial Services (63%) - Healthcare (59%) - Retail (56%)	- Phased rollout - User involvement in design - Change management programs - Executive sponsorship - Parallel operations
Data Quality Issues	49%	Poor data integrity impacting analytics, automation, and detection platforms	- Manufacturing (64%) - Government (57%) - Energy (53%)	- Data cleansing initiatives - Source system improvements - Data governance programs - Quality monitoring and feedback
Performance Impacts	43%	Security tools affecting system performance, UX, or transaction speed	- Financial Services (62%) - Retail (56%) - Technology (48%)	- Performance testing - System tuning - Deployment optimization - Lightweight agent design
Governance and Compliance	37%	Ensuring compliance with regulations and internal policies in new technology deployments	- Healthcare (58%) - Financial Services (53%) - Energy (45%)	- Early compliance involvement - Regulatory mapping - Compliance-by-design - Automated documentation

Source: Survey data (n = 156). Percentages reflect respondents identifying each challenge as significant or very significant. Sector data represents prevalence of the challenge within each industry segment.

Organizations reporting the most successful technology implementations demonstrated structured approaches including:

- Business case development with clearly defined success criteria
- Phased implementation with defined success metrics at each stage
- Cross-functional implementation teams including business stakeholders
- Structured change management and user adoption processes
- Continuous improvement cycles with regular reassessment

4.4. Sector-Specific Patterns in U.S. Risk Management

Analysis revealed significant variation in cyber risk management approaches across different sectors of the U.S. economy, reflecting diverse regulatory requirements, threat landscapes, operational constraints, and maturity levels.

4.4.1. Financial Services Sector

The U.S. financial services sector demonstrated the most mature cyber risk management practices among the industries studied. This sector faces a complex regulatory landscape including Gramm-Leach-Bliley Act requirements, NYDFS Cybersecurity Regulation, FFIEC guidance, and OCC standards.

Distinctive characteristics of financial sector approaches included:

- Comprehensive framework implementation combining regulatory requirements with voluntary standards (average 3.7 frameworks per organization)
- Sophisticated threat intelligence capabilities with sector-specific threat modeling
- Advanced detection and response capabilities with heavy automation investment

- Substantial third-party risk management programs reflecting supply chain concerns
- Board-level risk committees with dedicated cybersecurity expertise

A banking sector CISO described their approach:

"Our risk management program balances three imperatives regulatory compliance, threat-based security, and business enablement. We maintain a mature control environment mapped to multiple frameworks, but we're equally focused on threat intelligence and advanced detection. The regulatory requirements establish our baseline, but our program extends well beyond compliance to address the specific threats targeting financial institutions." (Participant 6, Financial Services)

Financial institutions reported the highest technology investment levels among sectors studied (average 14% of IT budget allocated to security) and the most advanced governance structures, with 82% reporting dedicated board risk committees with cybersecurity oversight.

4.4.2. Healthcare Sector

The healthcare sector demonstrated distinctive risk management patterns shaped by HIPAA requirements, patient safety concerns, and complex technology environments spanning traditional IT, clinical systems, and connected medical devices.

Key characteristics of healthcare approaches included:

- Strong emphasis on data protection controls reflecting HIPAA requirements
- Challenges balancing security with clinical operational requirements
- Significant legacy technology constraints limiting security implementation options
- Growing focus on medical device security and clinical network segmentation
- Increasing collaboration between security and clinical engineering functions

A healthcare security director explained their sector-specific challenges:

"Healthcare presents unique security challenges 24/7 operations where minutes matter for patient care, legacy clinical systems that can't be easily upgraded, and connected medical devices with 10-15 year lifecycles. Our approach emphasizes strong data protection per HIPAA but recognizes that we must balance security with clinical imperatives. We focus on defense-in-depth and compensating controls where we can't implement standard security measures due to clinical constraints." (Participant 19, Healthcare)

Healthcare organizations reported significant resource constraints compared to financial and technology sectors, with security budgets averaging 9% of IT spending. They also reported higher levels of security exceptions (average 36 active exceptions per organization) reflecting the challenges of securing complex clinical environments with patient care priorities.

4.4.3. Critical Infrastructure Sectors

Critical infrastructure sectors including energy, water, and transportation showed risk management approaches heavily influenced by operational technology (OT) considerations and increasing regulatory attention following recent high-profile incidents.

Distinctive characteristics included:

- Growing convergence of IT and OT security programs with unified governance
- Substantial focus on availability and reliability alongside confidentiality concerns
- Increasing adoption of industrial-specific frameworks and controls
- Significant collaboration with government agencies on threat intelligence
- Advanced incident response capabilities for cyber-physical incidents

An energy sector security leader described their evolving approach:

"Critical infrastructure security has transformed from primarily physical protection to a sophisticated cyber-physical approach. We've moved beyond air-gapped OT systems to acknowledge the reality of IT/OT convergence. Our risk management now spans traditional IT assets, operational technology, and industrial control systems under a unified governance model. We've developed specific security standards for each environment while maintaining consistent risk management processes across the organization." (Participant 25, Energy)

Critical infrastructure organizations reported increasing regulatory pressure following the Colonial Pipeline incident and subsequent executive orders, with 73% anticipating new compliance requirements within the next two years. These organizations were also most likely to report active participation in public-private partnerships for threat intelligence sharing (78% compared to 52% across all sectors).

4.4.4. Technology Sector

The U.S. technology sector demonstrated distinctive risk management approaches reflecting both advanced capabilities and unique challenges as both security consumers and providers.

Key characteristics included

- Security deeply integrated with development and engineering processes
- Strong emphasis on automation and security-as-code approaches
- Advanced application security programs with developer-focused tools
- Significant focus on supply chain security for both inputs and products
- Challenge of balancing innovation speed with security requirements

A technology company CISO described their sector-specific approach:

"As a technology provider, we face the dual challenge of securing our own environment while ensuring our products are secure for customers. Our risk management approach emphasizes integration into development processes secure by design, automated security testing, and continuous monitoring throughout the development lifecycle. We've moved beyond traditional security gates that slow innovation toward automated guardrails that enable secure development at speed." (Participant 14, Technology)

Technology organizations reported the highest levels of security automation (92% implementing SOAR platforms) and the most advanced DevSecOps practices, with 76% reporting "significant" or "comprehensive" integration of security into development processes.

4.5. The USA Cyber Risk Integration Framework

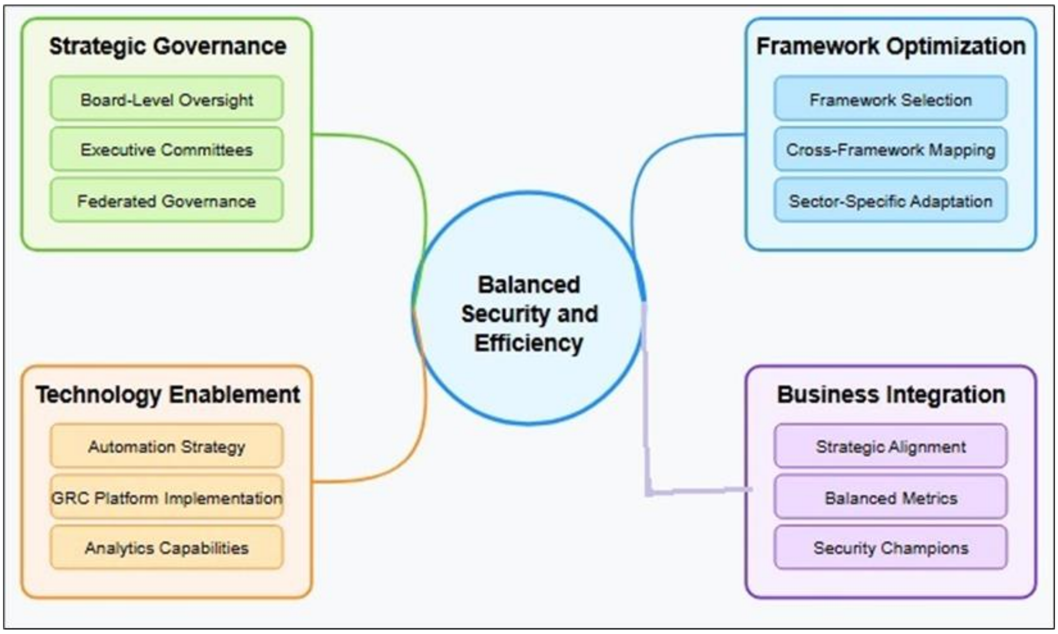


Figure 7 USA Cyber Risk Integration Framework

Building on the research findings, we developed a USA Cyber Risk Integration Framework that synthesizes effective approaches for balancing security and efficiency within the unique American regulatory and business context as shown figure 7. This framework addresses the distinctive characteristics of U.S. organizations while providing a structured approach for effective cyber risk management.

4.5.1. Framework Components

The USA Cyber Risk Integration Framework comprises five interconnected components, each addressing critical dimensions of balanced risk management:

Strategic Governance establishes the organizational structures and processes for aligning cybersecurity with business objectives and regulatory requirements. This component encompasses:

- Board-level oversight structures with appropriate expertise
- Executive steering committees with cross-functional representation
- Federated governance models balancing central oversight with business unit autonomy
- Structured risk acceptance and exception processes
- Clear delineation of security accountabilities across business functions

Framework Optimization addresses the selection, adaptation, and implementation of cybersecurity frameworks to meet organizational requirements while minimizing duplication and inefficiency. This component includes:

- Framework selection methodology based on regulatory and business requirements
- Mapping and harmonization across multiple frameworks
- Sector-specific adaptations and extensions
- Documentation approach supporting legal defensibility
- Maturity model for progressive implementation

Technology Enablement focuses on leveraging appropriate technologies to enhance risk management effectiveness while reducing operational friction. This component covers:

- Technology selection criteria aligned with risk priorities
- Automation strategy for high-volume, low-judgment activities
- Analytics capabilities supporting risk-based decision-making
- GRC platform implementation for streamlined compliance
- Identity and access solutions balancing security with usability

Business Integration addresses the alignment of security activities with business processes and objectives. This component encompasses:

- Security integration into business planning and strategic initiatives
- Balanced metrics addressing both security effectiveness and business impact
- Tailored security approaches for different business functions
- Security champions programs embedding expertise in business units
- Executive engagement model building security understanding

Continuous Adaptation enables ongoing evolution of the security program in response to changing threats, regulations, and business requirements. This component includes:

- Threat intelligence integration processes
- Regulatory horizon scanning capabilities
- Feedback mechanisms for operational impact assessment
- Performance measurement and program optimization
- Continuous improvement methodology

4.5.2. Implementation Approach

The framework is designed for iterative implementation, with organizations progressing through four phases of increasing maturity:

- **Phase 1: Foundation Building** focuses on establishing essential governance structures, implementing basic framework elements, and deploying foundational technologies. This phase creates the necessary infrastructure for effective risk management while addressing the most critical security gaps.
- **Phase 2: Optimization and Efficiency** emphasizes streamlining compliance activities, reducing redundancy across frameworks, and implementing automation for routine security processes. This phase significantly improves operational efficiency while maintaining security effectiveness.
- **Phase 3: Business Integration** addresses deeper alignment between security and business functions, with security controls and processes integrated into business workflows rather than operating as separate activities. This phase substantially improves the security-efficiency balance through thoughtful integration.
- **Phase 4: Strategic Enablement** positions security as a strategic business enabler rather than a compliance function, with security capabilities actively supporting business innovation and competitive advantage. This phase represents the highest maturity level, where security adds business value beyond risk reduction.

4.5.3. Sectoral Adaptations

- The framework includes specific adaptation guidance for different sectors of the U.S. economy, recognizing the distinctive requirements and constraints across industries:
- **Financial Services Adaptation** emphasizes integration across multiple regulatory frameworks, advanced threat intelligence capabilities, sophisticated third-party risk management, and alignment with business innovation initiatives.
- **Healthcare Adaptation** focuses on balancing HIPAA compliance with clinical operations, addressing medical device security challenges, implementing appropriate compensating controls for legacy systems, and aligning security with patient safety objectives.
- **Critical Infrastructure Adaptation** addresses IT/OT convergence challenges, availability-focused risk assessment, sector-specific threat modeling, and collaboration with government partners on intelligence and incident response.
- **Technology Sector Adaptation** emphasizes integration with development processes, product security considerations, supply chain risk management, and balancing innovation speed with security requirements.

4.5.4. Validation and Application

The framework was validated through expert review with 12 senior security leaders and pilot application in three organizations across different sectors. Initial results indicate that the framework provides practical guidance for organizations seeking to improve security-efficiency balance, with pilot organizations reporting enhanced stakeholder satisfaction, improved risk visibility, and reduced operational friction.

The framework proved particularly effective in helping organizations:

- Identify and address governance gaps inhibiting effective balance
- Streamline compliance activities across multiple frameworks
- Select and implement appropriate enabling technologies
- Develop more business-aligned security approaches

5. Discussion

5.1. The Evolution of U.S. Cyber Risk Management

Our findings reveal an ongoing transformation in how U.S. organizations approach cyber risk management. The traditional compliance-oriented model characterized by checklist approaches, technology-centric controls, and limited business integration is giving way to more sophisticated approaches that balance security imperatives with operational requirements.

This evolution reflects broader maturation of cybersecurity as a business function rather than a purely technical domain. As one participant observed:

"We've seen cybersecurity evolve from an IT sub-function focused on firewalls and antivirus to a true enterprise risk management discipline with board visibility and business integration. This evolution parallels the transformation of other business functions like quality management, which similarly progressed from technical specialization to enterprise-wide management system." (Participant 1, Financial Services)

The research indicates that this transformation occurs along multiple dimensions simultaneously:

- Governance Evolution: From IT-dominated committees to cross-functional bodies with executive and board representation
- Framework Implementation: From strict compliance approaches to risk-based adaptation and business integration
- Technology Adoption: From point solutions addressing specific threats to integrated platforms enabling comprehensive risk management
- Organizational Positioning: From technical support function to strategic business partner

Organizations further in this evolution demonstrate significantly better security-efficiency balance, suggesting that maturation naturally addresses many traditional tensions between security and operations.

5.2. The Distinctive American Approach

The research highlights several characteristics that distinguish U.S. cyber risk management approaches from international patterns described in the literature. These distinctive elements reflect the unique American regulatory landscape, business culture, and technological environment.

5.2.1. Legal and Regulatory Influences

The fragmented U.S. regulatory landscape significantly shapes risk management approaches. Unlike jurisdictions with comprehensive cybersecurity legislation, U.S. organizations must navigate sector-specific regulations, state-level requirements, and the implicit obligations created through litigation and enforcement actions.

This environment creates what one participant termed "compliance ambiguity" where organizations lack clear, comprehensive standards but face potential liability for security failures. This ambiguity has driven the strong adoption of voluntary frameworks as de facto standards for reasonable security. As a financial services attorney observed:

"The U.S. lacks a single, comprehensive cybersecurity law, but that doesn't mean organizations operate without obligations. The combination of sectoral regulations, FTC enforcement, state laws, and the common law duty of care creates significant compliance requirements. Voluntary frameworks like the NIST CSF provide a structured approach to navigate this complex landscape while establishing legal defensibility." (Participant 35, Legal Expert)

This legal environment particularly influences documentation practices, with U.S. organizations demonstrating more extensive documentation of risk decisions, control implementations, and security governance than described in international studies. This documentation serves both operational and legal purposes, creating an audit trail for potential regulatory investigations or litigation.

5.2.2. The Federated Implementation Model

The research revealed what appears to be a distinctly American approach to implementation through federated governance models. This approach balances central oversight with significant business unit autonomy reflecting broader American corporate culture that values decentralized decision-making and business unit accountability.

This model differs from both the centralized approaches common in European organizations and the highly decentralized approaches sometimes observed in Asian conglomerates. As one multinational security leader explained:

"In our European operations, we see more centralized security functions with stronger authority over business units. In our Asian operations, security is often highly decentralized with limited enterprise standards. Our U.S. approach sits between these extremes we establish enterprise requirements and maintain central visibility, but business units have significant implementation flexibility within those guardrails." (Participant 30, Manufacturing)

The federated model appears particularly well-suited to the U.S. business environment, allowing organizations to maintain consistent security posture while accommodating the operational diversity and autonomy valued in American corporate culture.

5.2.3. Technology Orientation

U.S. organizations demonstrate stronger orientation toward technological solutions compared to international patterns described in the literature. This reflects both higher technology investment levels and the American business preference for addressing challenges through automation rather than process or organizational changes alone.

The research revealed particularly high adoption of security automation, analytics platforms, and integrated GRC solutions compared to international benchmarks. As one technology vendor observed:

"U.S. organizations consistently lead global adoption of advanced security technologies. This reflects both higher security budgets and a cultural preference for technological solutions. American enterprises typically ask 'what technology can solve this problem?' before considering process or organizational approaches. This creates both opportunities and challenges for balanced risk management." (Participant 34, Technology Provider)

While this technology orientation creates opportunities for efficiency gains, the research also revealed potential pitfalls when technology implementation occurs without appropriate governance, process integration, and change management. Organizations achieving the best security-efficiency balance demonstrated thoughtful integration of technology with governance structures and business processes rather than viewing technology as a standalone solution.

5.3. Framework Effectiveness and Adaptation

The research provides important insights on the effectiveness of voluntary frameworks in the U.S. context and how organizations adapt these frameworks to their specific requirements. The findings challenge simplistic views of frameworks as rigid compliance checklists, instead revealing sophisticated adaptation practices that maintain framework benefits while addressing organizational needs.

5.3.1. From Compliance to Risk Management

The most effective organizations demonstrated evolution from compliance-oriented framework implementation toward risk-based approaches. This transition involves shifting from viewing framework requirements as compliance obligations toward seeing them as tools for effective risk management.

A financial services risk officer described this evolution:

"We initially implemented the NIST CSF as a compliance exercise, focusing on documentation and gap assessments. As we matured, we recognized that the true value comes from using the framework as a risk management tool identifying our most significant risks and prioritizing controls that address those specific concerns. The framework became a means rather than an end, guiding our risk management rather than defining it." (Participant 7, Financial Services)

Organizations further in this evolution reported both better security outcomes (mean rating 4.3/5 vs. 3.2/5) and greater operational efficiency (mean rating 4.1/5 vs. 2.9/5) compared to those maintaining compliance-oriented approaches.

5.3.2. Hybrid Farmwork Approaches

The research revealed sophisticated practices for combining elements from multiple frameworks to address diverse requirements while minimizing duplication. U.S. organizations face particular challenges in this area given the sectoral regulatory approach and overlapping framework requirements.

Effective organizations addressed this challenge through framework mapping and harmonization creating unified control frameworks that satisfy multiple requirements simultaneously. As a healthcare security director explained:

"We created a unified control framework by mapping HIPAA, NIST CSF, HITRUST, and state requirements to a common set of controls. This consolidated approach lets us satisfy all requirements through a single implementation effort rather than maintaining separate compliance programs. We can demonstrate compliance with any framework while maintaining a cohesive security program." (Participant 20, Healthcare)

Organizations implementing unified control frameworks reported significant efficiency improvements, with average reductions of 37% in compliance assessment efforts and 42% in documentation activities.

5.3.3. Framework Extension Practices

The research identified sophisticated practices for extending standard frameworks to address emerging risks and specific organizational requirements. These extensions enable organizations to maintain framework alignment while addressing gaps in standard frameworks.

5.3.4. Common extension areas included:

- Cloud security controls beyond those in standard frameworks
- Supply chain security requirements reflecting recent compromises
- Machine learning and AI governance addressing emerging technologies
- Remote work security addressing pandemic-driven workplace changes
- Integration of privacy requirements alongside security controls
- A technology sector CISO described their extension approach:

"We maintain alignment with the NIST CSF for our core security program, but we've extended it in several areas where the standard framework lacks depth. We've added detailed cloud security controls based on the Cloud Security Alliance framework, developed comprehensive supply chain security requirements beyond those in standard frameworks, and integrated machine learning governance into our risk management approach. These extensions address our specific risk profile while maintaining the benefits of framework alignment." (Participant 16, Technology)

Organizations implementing thoughtful framework extensions reported better alignment with business-specific risks (mean rating 4.4/5) compared to those strictly implementing standard frameworks without adaptation (3.2/5).

5.4. The Technology-Efficiency Relationship

The research provides important insights into the relationship between technology implementation and security-efficiency balance. While technology represents a critical enabler of efficient risk management, the findings reveal more complex relationships than simple technology adoption driving improved outcomes.

5.4.1. Beyond Automation to Transformation

Organizations achieving the greatest efficiency improvements demonstrated approaches that went beyond simple task automation to fundamentally transform security processes. Rather than automating existing processes, these organizations redesigned workflows to leverage technology capabilities effectively.

A technology sector security leader explained:

"The organizations getting the most from security automation aren't just replacing manual tasks with automated ones. They're fundamentally rethinking security processes based on what technology enables. Rather than automating an inefficient manual vulnerability management process, they're implementing continuous assessment with automated prioritization and orchestrated remediation a completely different approach enabled by technology." (Participant 14, Technology)

This distinction between automation and transformation helps explain why some organizations report modest benefits from technology investments while others achieve dramatic improvements. Those approaching technology as a catalyst for process transformation reported substantially greater efficiency gains (average 47% improvement) compared to those focusing solely on task automation (24%).

5.4.2. The Human-Technology Balance

The research revealed important insights about the relationship between technology implementation and human expertise. The most effective organizations demonstrated thoughtful approaches to determining which activities benefit from automation versus human judgment.

A financial services CISO described their approach:

"We've developed a structured framework for deciding what to automate versus what requires human expertise. Routine, repeatable tasks with clear decision criteria are automated, freeing our analysts for activities requiring judgment, creativity, and contextual understanding. This isn't about replacing people with technology it's about focusing human expertise where it adds the most value while letting technology handle routine activities." (Participant 5, Financial Services)

Organizations with clear strategies for human-technology balance reported better security outcomes (mean rating 4.5/5) compared to those with either minimal automation or attempts to automate complex judgment activities (3.3/5).

5.4.3. Implementation Success Factors

The research identified several factors that distinguish successful technology implementations from those that fail to deliver expected benefits. Critical success factors included:

- Executive sponsorship with clear business objectives beyond technical metrics
- Cross-functional implementation teams including business stakeholders
- Phased deployment approaches with clear success criteria at each stage
- Investment in user experience and change management
- Skills development aligned with technology implementation
- Regular reassessment and continuous improvement processes

Organizations addressing these factors comprehensively reported significantly higher satisfaction with technology implementations (mean rating 4.4/5) compared to those focusing primarily on technical aspects (2.7/5).

5.5. Implications for Practice

Our findings have several important implications for cybersecurity practitioners, technology vendors, and policymakers in the U.S. context:

- Security Leaders should prioritize the development of federated governance models that balance central oversight with business unit autonomy. These models align particularly well with American corporate cultures while enabling consistent security with appropriate flexibility.
- Risk Management Teams should focus on framework harmonization rather than maintaining separate compliance programs for different requirements. Unified control frameworks mapped to multiple standards significantly improve efficiency while maintaining comprehensive coverage.
- Technology Executives should approach security technology as a catalyst for process transformation rather than simply automating existing activities. The greatest efficiency gains come from fundamentally redesigning security processes to leverage technology capabilities.
- Board Members should ensure appropriate oversight structures for cybersecurity, recognizing that traditional approaches through audit committees may be insufficient for complex cyber risks. Dedicated risk committees or specialized expertise on existing committees enhance oversight effectiveness.
- Policymakers should recognize the effectiveness of the voluntary standards model in the U.S. context while seeking opportunities to reduce regulatory fragmentation. The research supports the value of framework flexibility while highlighting the compliance challenges created by overlapping requirements.
- The USA Cyber Risk Integration Framework proposed in this research offers organizations a structured approach for implementing these recommendations, providing practical guidance for achieving appropriate security-efficiency balance within the unique American business and regulatory environment.

5.6. Limitations and Future Research

This study has several limitations that suggest directions for future research. First, while the sample included organizations across multiple sectors and sizes, it predominantly represented medium and large enterprises with established security programs. Future research should examine security-efficiency balance in smaller organizations with more limited resources.

Second, while the research identified distinctive patterns in U.S. organizations, it did not include direct international comparisons within the same study. Comparative research explicitly examining differences between U.S. and international approaches would provide valuable additional insights.

Third, the study provides a snapshot of current practices but offers limited longitudinal perspective on how approaches evolve over time. Future research tracking organizations through their security maturation journey would enhance understanding of how security-efficiency balance develops.

- Several specific areas warrant further investigation:
- Examining the effectiveness of different board oversight structures for cybersecurity governance
- Exploring the organizational and cultural factors that influence technology adoption and effectiveness
- Investigating how smaller organizations without dedicated security resources achieve appropriate security-efficiency balance
- Analyzing the impact of emerging privacy regulations on integrated security and privacy risk management

These research directions would build upon the findings presented here to develop more comprehensive understanding of how organizations can effectively balance security requirements with operational imperatives in the unique American business environment.

6. Conclusion

This research investigated how U.S. organizations balance security and efficiency through the application of voluntary standards and emerging technologies within cyber risk management frameworks. Through a mixed-methods approach combining qualitative interviews with cybersecurity leaders and quantitative survey data, we examined framework implementation practices, governance structures, technology utilization, and sector-specific patterns across diverse organizations.

The findings reveal distinctive characteristics of U.S. approaches to cyber risk management, including sophisticated framework adaptation practices, federated governance models balancing central oversight with business unit autonomy, high technology adoption with emphasis on automation and analytics, and significant variation across industry sectors reflecting the fragmented regulatory landscape.

The research demonstrates that organizations achieving optimal security-efficiency balance share several characteristics: they implement frameworks as risk management tools rather than compliance checklists, establish cross-functional governance structures with appropriate executive engagement, leverage technologies to transform security processes rather than simply automating existing activities, and integrate security considerations into business workflows rather than operating as separate functions.

Based on these findings, we developed the USA Cyber Risk Integration Framework that synthesizes effective approaches for balancing security and efficiency within the unique American context. This framework addresses the distinctive characteristics of U.S. organizations while providing a structured approach for implementing effective risk management practices.

As cyber threats continue to evolve and digital transformation reshapes business operations, the ability to implement effective security without creating undue operational friction becomes increasingly critical. This research contributes to both scholarly understanding and practical implementation of balanced cyber risk management approaches in the distinctive American business and regulatory environment.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Alozie, C. E., & Chinwe, E. E. (2025). Developing a Cybersecurity Framework for Protecting Critical Infrastructure in Organizations. ICONIC RESEARCH AND ENGINEERING JOURNALS, 8(7), 562–576. https://doi.org/10.5281/zenodo.14740463

[2] Alozie, C. E. (2024). Threat modeling in the health care sector. ResearchGate. Retrieved from https://www.researchgate.net/publication/380151256_Beyond_Conventional_Threat_DefenseImplementing_Advanced_Threat_Modeling_Techniques_Risk_Modeling_Frameworks_and_Contingency_Planning_in_the_Healthcare_Sector_for_Enhanced_Data_Security

[3] Ajayi, O. O., Alozie, C. E., & Abieba, O. A. (2025). Enhancing cybersecurity in energy infrastructure: Strategies for safeguarding critical systems in the digital age. Trends in Renewable Energy. Retrieved from futureenergysp.com

[4] Ajayi, O. O., Alozie, C. E., Abieba, O. A., Akerele, J. I., & Collins, A. (2025). Blockchain technology and cybersecurity in fintech: Opportunities and vulnerabilities. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 11(1), 1–10. https://doi.org/10.32628/CSEIT25111210IJSRCSEIT

[5] Folorunso, O. (2023). Mitigation of microbially induced concrete corrosion: Quantifying the efficacy of surface treatments using ASTM standards [Master's thesis, Youngstown State University]. Civil and Environmental Engineering Program.

[6] Akinbolajo, O. (2024). The role of technology in optimizing supply chain efficiency in the American manufacturing sector. International Journal of Humanities Social Science and Management (IJHSSM), 4(2), 530–539.

[7] Chidozie et al. (2025). Quantum Computing and its Impact on Cryptography: The Future of Secure Communications and Post-Quantum Cryptography. 3. 10.5281/zenodo.15148534.

[8] Egbedion Grace et al. (2025). Securing Internet of Things (IoT) ecosystems: Addressing scalability, authentication, and privacy challenges. World Journal of Advanced Research and Reviews. 523-534. 10.30574/wjarr.2025.26.1.0999.

[9] Bamberger, K. A., & Mulligan, D. K. (2019). Cybersecurity governance: Public-private partnerships and standardization in the United States. In D. Carpenter & D. Moss (Eds.), Cambridge Handbook of Technical Standardization Law (pp. 323-345). Cambridge University Press.

[10] Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77-101.

[11] Caimi, G., Boehm, J., Calkins, M., & Palacios, G. (2021). Digital and technology transformation: A CEO agenda. McKinsey & Company.

[12] Carr, M. (2016). Public-private partnerships in national cyber-security strategies. International Affairs, 92(1), 43-62.

[13] Chen, Y., & Gupta, A. (2021). Cybersecurity governance in large U.S. enterprises: A systematic analysis of board involvement and reporting structures. Journal of Cybersecurity, 7(1), tyab002.

[14] Chinwe, E. E., & Alozie, C. E. (2025). Adversarial Tactics, Techniques, and Procedures (TTPs): A Deep Dive into Modern Cyber Attacks. ICONIC RESEARCH AND ENGINEERING JOURNALS, 8(7), 552–561. https://doi.org/10.5281/zenodo.14740424

[15] Creswell, J. W., & Plano Clark, V. L. (2018). Designing and conducting mixed methods research (3rd ed.). SAGE Publications.

[16] Deloitte. (2021). The future of cyber survey 2021. Deloitte Insights.

[17] Financial Services Information Sharing and Analysis Center (FS-ISAC). (2021). Navigating cyber 2021: A report on the global financial system's cyber landscape. FS-ISAC.

[18] Forrester Research. (2022). Global security budgets 2022: Regional and industry variations. Forrester Research, Inc.

[19] Friedberg, I., & Skopik, F. (2021). Cybersecurity framework adaptation for critical infrastructure providers. Journal of Infrastructure Protection and Resilience, 1(2), 183-201.

[20] Gartner. (2023). Forecast analysis: Information security and risk management, worldwide. Gartner, Inc.

[21] Government Accountability Office (GAO). (2022). Cybersecurity: Federal agencies need to implement recommendations to manage supply chain risks (GAO-22-105007). U.S. Government Printing Office.

[22] Guetterman, T. C., Fetters, M. D., & Creswell, J. W. (2015). Integrating quantitative and qualitative results in health science mixed methods research through joint displays. Annals of Family Medicine, 13(6), 554-561.

[23] Healthcare Information and Management Systems Society (HIMSS). (2022). 2022 HIMSS cybersecurity survey. HIMSS.

[24] Hoffman, J., & Ramakrishna, S. (2022). Integrated risk governance: A model for financial institutions. Journal of Risk Management in Financial Institutions, 15(2), 178-193.

[25] Industrial Control Systems Joint Working Group. (2021). Control systems defense in industrial environments. Cybersecurity and Infrastructure Security Agency.

[26] Information Technology Industry Council. (2020). Framework for improving critical infrastructure cybersecurity: Industry implementation. Information Technology Industry Council.

[27] Johnson, C., Badger, L., Waltermire, D., Snyder, J., & Skorupka, C. (2020). Cybersecurity framework voluntary implementation experiences from U.S. organizations (NIST Technical Note 2051). National Institute of Standards and Technology.

[28] Kosseff, J. (2018). Defining cybersecurity law. Iowa Law Review, 103(3), 985-1032.

[29] McAfee. (2021). Enterprise security architecture: Industry perspective 2021. McAfee, LLC.

[30] Morgan, K. D., & Chess, B. (2020). Modifying security frameworks for application in specific sectors. IEEE Security & Privacy, 18(3), 40-49.

[31] National Cyber Security Alliance. (2022). 2022 state of cybersecurity in small and medium-sized businesses. National Cyber Security Alliance.

[32] National Institute of Standards and Technology (NIST). (2018). Framework for improving critical infrastructure cybersecurity, Version 1.1. U.S. Department of Commerce.

[33] Schwartz, P. M., & Peifer, K.-N. (2017). Transatlantic data privacy law. Georgetown Law Journal, 106(1), 115-179.

[34] Shackleford, D. (2021). 2021 SANS automation and integration survey. SANS Institute.

[35] Shen, Y. (2022). Governance by executive order: The evolution of U.S. cyber policy. Journal of Information Technology & Politics, 19(3), 289-306.

[36] Tran, H. (2021). Critical infrastructure cybersecurity: Evaluating the adequacy of public-private partnerships. Journal of Homeland Security and Emergency Management, 18(2), 147-168.

[37] Verma, S., & Domingos, C. (2021). The checkbox compliance trap: Understanding the limitations of framework-driven cybersecurity. Journal of Information Security and Applications, 61, 102941.

[38] White House. (2021). Executive Order 14028: Improving the nation's cybersecurity. Federal Register, 86(93), 26633-26647.

[39] Wolff, J. (2018). You'll see this message when it is too late: The legal and economic aftermath of cybersecurity breaches. MIT Press.

[40] Zhang, L., & Rodriguez, M. (2021). Application of artificial intelligence in U.S. financial sector cybersecurity. Financial Markets, Institutions & Instruments, 30(3), 95-123.