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)

Check for updates

Balancing efficiency and security: The role of voluntary standards and emerging technologies in cyber risk management framework in the global space

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

[1] *Department of Information Technology University of the cumberlands,Kentucky , United States.*
[2] *Department of Satish & Yasmin Gupta College of Business Institution, University of Dallas USA.*

World Journal of Advanced Research and Reviews, 2025, 26(02), 2411-2433

Publication history: Received on 04April 2025; revised on 13 May 2025; accepted on 15 May 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.26.2.1896

Abstract

This research investigates the evolving balance between operational efficiency and security controls in global cyber risk management frameworks. Through a mixed-methods approach combining quantitative survey data from 183 organizations across 27 countries and qualitative insights from 42 in-depth interviews with cybersecurity leaders, the study examines how voluntary standards and emerging technologies shape contemporary risk management practices. Findings reveal that organizations achieving optimal security-efficiency balance demonstrate three key characteristics: integrated risk governance structures, dynamic adaptation of voluntary frameworks, and strategic implementation of automation technologies. The research identifies significant variations in framework adoption across different regions, with harmonization challenges stemming from regulatory fragmentation, organizational maturity disparities, and technological capability gaps. A novel "Adaptive Security-Efficiency Model" is proposed, offering organizations a structured approach to calibrating security controls with operational needs while remaining responsive to evolving threat landscapes. This study contributes to both scholarly understanding and practical implementation of balanced cyber risk management in an increasingly complex global environment.

Keywords: Cyber Risk Management; Voluntary Standards; Emerging Technologies; Operational Efficiency; Global Harmonization; Security Automation; Risk Governance

1. Introduction

1.1. The Security-Efficiency Dilemma

Organizations across the global digital ecosystem face an increasingly complex challenge: maintaining robust cybersecurity postures while simultaneously preserving operational efficiency and business agility. This tension has intensified as cyber threats have become more sophisticated, regulatory requirements more stringent, and business processes more digitally dependent (Jang-Jaccard & Nepal, 2014). The traditional security paradigm often emphasized defensive controls that, while potentially effective at risk reduction, frequently created operational friction, reduced productivity, and hindered innovation (Libertini et al., 2021).

Recent high-profile security incidents—from the SolarWinds supply chain compromise to the Colonial Pipeline ransomware attack—have further amplified the stakes of inadequate security. Simultaneously, the COVID-19 pandemic accelerated digital transformation timelines, creating additional pressure to balance security with the operational demands of rapidly evolving business models (Georgiadou et al., 2022). Organizations increasingly recognize that neither maximum security at the expense of operations nor minimal security in service of efficiency represents a sustainable approach.

*Corresponding author: CHISOM ELIZABETH ALOZIE

1.2. The Role of Voluntary Standards

Against this backdrop, voluntary cybersecurity standards and frameworks have emerged as critical tools for organizations seeking to implement structured, comprehensive risk management approaches. Frameworks such as the NIST Cybersecurity Framework (CSF), ISO 27001, and the Center for Internet Security (CIS) Controls provide structured guidance that can be adapted to various organizational contexts (NIST, 2018; ISO/IEC, 2022; CIS, 2021).

These voluntary standards offer several potential advantages: they represent collective expertise, provide common terminology and metrics, enable cross-organizational comparison, and can support compliance with regulatory requirements (Pham et al., 2022). However, questions remain about their practical implementation, particularly regarding how organizations can adapt these standards to achieve appropriate balance between security and operational requirements within their specific contexts.

1.3. Emerging Technologies in Risk Management

Concurrent with the evolution of voluntary standards, emerging technologies are transforming cyber risk management practices. Artificial intelligence and machine learning, robotic process automation, advanced analytics, and security orchestration platforms increasingly offer capabilities that may help resolve the security-efficiency dilemma (Shafiq et al., 2021). These technologies potentially enable more accurate risk assessment, automated compliance verification, intelligent threat detection, and streamlined security operations.

However, technological solutions also introduce new complexities, including implementation challenges, potential dependencies, and in some cases, novel security risks of their own (Mariani et al., 2022). The actual contribution of these technologies to balanced risk management remains under-examined in the scholarly literature, particularly regarding their integration with established frameworks and standards.

1.4. The Global Harmonization Challenge

The challenge of balancing security and efficiency is further complicated in the global context, where organizations must navigate diverse regulatory requirements, varying threat landscapes, and different cultural approaches to risk management (van der Kleij et al., 2017). While voluntary standards often aim to establish common practices across borders, significant regional variations persist in both regulatory requirements and implementation approaches.

These variations create particular challenges for multinational organizations, which must implement coherent risk management approaches while addressing location-specific requirements. They also present obstacles to global collaboration on cybersecurity, potentially creating vulnerabilities where approaches fail to align (Rodríguez-Vidal et al., 2023).

1.5. Research Objectives and Questions

This research aims to investigate how organizations can effectively balance security and efficiency through the application of voluntary standards and emerging technologies within cyber risk management frameworks. The study is guided by four primary research questions:

- How do organizations adapt voluntary cybersecurity standards to achieve appropriate security-efficiency balance within their specific operational contexts?
- What role do emerging technologies play in enabling more efficient and effective implementation of cyber risk management frameworks?
- What organizational governance structures and processes support optimal integration of security controls with business operations?
- How can global harmonization of cyber risk management approaches be advanced despite regional regulatory and cultural variations?

By addressing these questions, this research seeks to contribute both theoretical understanding and practical guidance for organizations navigating the complex balance between security imperatives and operational requirements in an increasingly challenging global environment.

2. Literature Review

2.1. Evolution of Cyber Risk Management Frameworks

Cyber risk management frameworks have evolved considerably over the past two decades, transitioning from compliance-oriented, checklist-based approaches toward more dynamic, risk-based methodologies. Early frameworks often emphasized technical controls and perimeter defense, reflecting the security paradigms of their era (von Solms & van Niekerk, 2013). Contemporary frameworks increasingly recognize cybersecurity as an enterprise risk management concern requiring integration with broader business processes and strategic decision-making (Hsu et al., 2021).

This evolution reflects growing recognition that effective cybersecurity requires more than technical controls—it demands consideration of organizational factors, human elements, and business context. Researchers have documented this transition from first-generation frameworks focused primarily on technical safeguards to third-generation approaches emphasizing risk-based decision-making, continuous adaptation, and business alignment (Ramirez & Kibel, 2020).

Despite this evolution, significant research gaps remain regarding how frameworks can effectively balance security rigor with operational flexibility, particularly in rapidly changing technological environments. As Pham et al. (2022) note, "theoretical models frequently assume ideal implementation conditions that rarely exist in organizational practice" (p. 247), highlighting the need for research that addresses real-world implementation challenges.

2.2. Security-Efficiency Balance in Organizational Contexts

The tension between security controls and operational efficiency has received increasing scholarly attention. Research by Kunnathur (2015) introduced the concept of "security friction," quantifying the operational impact of security measures in terms of workflow disruption, time costs, and user satisfaction. Subsequent studies have examined this friction in various contexts, including healthcare information systems (Jalali et al., 2020), critical infrastructure (Ibrahim & Kant, 2020), and financial services (Morris et al., 2021).

Several studies have attempted to quantify both the costs and benefits of security controls, with Talaoui and Kohtamäki (2022) proposing a "security equilibrium model" that seeks optimal balance points between security investment and operational impact. However, as they acknowledge, establishing meaningful metrics for this balance remains challenging, particularly given the difficulty of quantifying security benefits in the absence of incidents.

The literature reveals a gradual shift from viewing security and efficiency as inherently oppositional toward recognizing potential synergies when security is thoughtfully integrated into business processes. Libertini et al. (2021) describe this as "security by design" versus "security by addition," noting that retrofitted security controls typically create significantly more operational friction than those integrated during process design.

2.3. Voluntary Standards Implementation and Adaptation

Voluntary standards play an increasingly central role in cyber risk management, with widespread adoption of frameworks such as the NIST CSF, ISO 27001, and CIS Controls. Research has examined both the diffusion of these standards and their adaptation in various contexts. Diffusion studies indicate uneven adoption patterns, with larger organizations and those in highly regulated industries demonstrating higher implementation rates (Vejačka&Štofa, 2021).

Studies of framework adaptation reveal significant variation in implementation approaches. Some organizations apply frameworks comprehensively, while others adopt more selective approaches, implementing specific elements that align with their perceived risks and operational constraints (Mwenya & Ali, 2019). Several researchers have explored factors influencing these adaptation decisions, identifying variables including organizational size, industry sector, regulatory requirements, and resource availability (Anderson et al., 2021).

An emerging stream of research examines how organizations combine elements from multiple frameworks to create hybrid approaches tailored to their specific needs. Simonet and Green (2021) documented this "framework fusion" process in multinational organizations, noting that it often reflects attempts to address varied regulatory requirements while maintaining operational consistency. However, they also identified challenges in this approach, including potential gaps, control duplication, and increased complexity.

2.4. Technology-Enabled Risk Management

Emerging technologies are significantly reshaping cyber risk management practices, with particular attention to artificial intelligence, automation, and advanced analytics. Several studies have examined the application of machine learning algorithms to threat detection and vulnerability management, with evidence suggesting potential improvements in both effectiveness and efficiency compared to traditional approaches (Mahdavifar et al., 2021).

Research on security automation has documented efficiency gains in areas including vulnerability scanning, security testing, and incident response (Shaw et al., 2020). These studies generally indicate positive outcomes in terms of reduced response times, increased coverage, and improved consistency. However, as Romano et al. (2022) observe, automation benefits may be contingent on organizational maturity and appropriate implementation approaches.

Advanced analytics and visualization tools have received attention for their potential to improve risk assessment and communication. Studies by Zheng et al. (2021) and Kolini and Janczewski (2022) examined how these technologies can enhance understanding of complex risk scenarios and support more informed decision-making across both technical and non-technical stakeholders.

While the literature generally suggests that emerging technologies can contribute to both security and efficiency, multiple researchers have noted the lack of comprehensive frameworks for evaluating and selecting appropriate technological solutions within organizational risk management programs (Mariani et al., 2022).

2.5. Global Harmonization Challenges

Research on global cybersecurity harmonization has examined both the drivers of regional variation and potential approaches to greater alignment. Studies have identified multiple sources of variation, including different legal traditions, cultural approaches to risk, economic development levels, and geopolitical considerations (van der Kleij et al., 2017).

Regulatory fragmentation has received particular attention, with researchers documenting proliferation of cybersecurity regulations across jurisdictions and the resulting compliance challenges for multinational organizations (Dykstra & Spafford, 2018). Several studies have attempted to map these regulatory variations and their implications for global organizations, with Kuner et al. (2017) identifying more than 120 distinct national cybersecurity regulatory frameworks with varied requirements.

Efforts toward harmonization have been examined from multiple perspectives, including international standards development, regional collaboration initiatives, and global governance mechanisms. Rodríguez-Vidal et al. (2023) evaluated the effectiveness of various harmonization approaches, concluding that convergence around common principles rather than identical requirements may represent the most viable path forward given the persistence of regional variations.

2.6. Research Gaps

Despite the growing literature on cyber risk management frameworks, significant research gaps remain. First, while numerous studies have examined framework adoption, relatively few have investigated how organizations adapt frameworks to achieve appropriate security-efficiency balance within their specific contexts. Second, research on the role of emerging technologies in risk management has typically focused on specific applications rather than their integration with comprehensive frameworks. Third, the literature lacks robust models for evaluating and optimizing security-efficiency balance across different organizational environments. Finally, empirical research on global harmonization approaches remains limited, with few studies examining how organizations actually navigate regional variations in practice.

This research aims to address these gaps through a mixed-methods investigation of how organizations balance security and efficiency through the integration of voluntary standards and emerging technologies within their cyber risk management frameworks.

3. Methodology

3.1. Research Design

This study employed a sequential mixed-methods design to investigate how organizations balance security and efficiency in cyber risk management. The research followed an exploratory sequential approach (Creswell & Plano Clark, 2018), beginning with qualitative interviews to develop in-depth understanding of implementation approaches, followed by a quantitative survey to assess broader patterns and relationships.

This design was selected for its ability to leverage complementary strengths of qualitative and quantitative methods: the qualitative phase provided rich contextual insights into organizational practices and decision-making processes, while the quantitative phase enabled testing of emerging patterns across a larger, more diverse sample. The sequential approach allowed findings from the initial qualitative phase to inform development of the quantitative instrument, enhancing its relevance and validity.

3.2. Qualitative Phase

3.2.1. Sampling Strategy

The qualitative phase employed purposive sampling to identify cybersecurity leaders with substantial experience implementing risk management frameworks. Participants were selected to ensure diversity across several dimensions:

- Geographic regions (North America, Europe, Asia-Pacific, Latin America, Middle East/Africa)
- Industry sectors (including financial services, healthcare, manufacturing, technology, public sector)
- Organizational size (ranging from mid-sized organizations to global enterprises)
- Framework experience (including NIST CSF, ISO 27001, CIS Controls, and regional frameworks)

The final sample included 42 participants representing 38 organizations across 17 countries. Participants held senior roles including Chief Information Security Officers (CISOs), Security Directors, Risk Management Leaders, and Compliance Officers.

3.2.2. Data Collection

Semi-structured interviews were conducted between September 2022 and February 2023. The interview protocol addressed four primary domains: (1) framework selection and adaptation approaches, (2) security-efficiency balancing strategies, (3) technology integration within risk management processes, and (4) navigation of regional variations in requirements.

Interviews averaged 75 minutes in duration (range: 45-120 minutes) and were conducted via video conferencing platforms. All interviews were recorded with participant consent and professionally transcribed. Field notes documenting key observations and emerging themes supplemented the transcript data.

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 (25%) to establish coding consistency (Cohen's $\kappa = 0.84$). The coding framework combined inductive and deductive elements, with initial codes reflecting the research questions while allowing for emergent themes.

Analysis proceeded through several iterations of code refinement, theme development, and cross-case comparison. Developing themes were validated through member checking with six participants, who reviewed preliminary findings and provided feedback on interpretations.

3.3. Quantitative Phase

3.3.1. Survey Instrument Development

The survey instrument was developed based on findings from the qualitative phase combined with existing literature. The instrument contained 42 items addressing key dimensions identified in the qualitative analysis, including:

- Framework adoption and adaptation (8 items)

- Security-efficiency balance approaches (10 items)
- Governance structures and processes (7 items)
- Technology integration (9 items)
- Regional harmonization challenges (8 items)

Items employed 5-point Likert scales, multiple choice selections, and ranking questions. The instrument underwent expert review by four cybersecurity professionals and was pilot tested with 12 respondents to assess clarity, relevance, and completion time. Refinements based on pilot feedback improved item wording and response option clarity.

3.3.2. Sampling and Data Collection

The survey was distributed to cybersecurity and risk management professionals between March and July 2023. Distribution channels included professional associations (International Information System Security Certification Consortium, Information Systems Security Association, ISACA), industry forums, and professional networks. The survey was offered in English, Spanish, Mandarin, and French to enhance accessibility across regions.

A total of 214 responses were received, with 183 complete responses retained for analysis after excluding partial submissions and those failing attention check questions. The final sample included respondents from 27 countries across 16 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 to examine relationships between key variables, analysis of variance (ANOVA) to compare responses across groups, and multiple regression to identify predictors of effective security-efficiency balance.

Principal component analysis was employed to identify underlying factors in approaches to framework adaptation and security-efficiency balance. Reliability analysis confirmed acceptable internal consistency for multi-item scales (Cronbach's α ranging from 0.74 to 0.92).

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 potential divergences requiring further examination.

Particular attention was given to how quantitative results expanded upon, clarified, or qualified insights from the qualitative phase. The integrated analysis formed the basis for development of the Adaptive Security-Efficiency Model presented in the findings.

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.

4. Findings

4.1. Framework Adaptation and Implementation

Analysis of both qualitative and quantitative data revealed diverse approaches to the adoption and adaptation of voluntary cybersecurity frameworks. While 89% of survey respondents reported using at least one voluntary framework, implementation approaches varied significantly in terms of comprehensiveness, adaptation strategies, and integration with business processes.

Table 1 Framework Adoption Rates by Region

Framework	Global Average	North America	Europe	Asia-Pacific	Middle East/Africa	Latin America
NIST Cybersecurity Framework	68%	77%	54%	62%	48%	51%
ISO 27001	63%	52%	78%	71%	59%	47%
CIS Controls	42%	51%	38%	35%	31%	29%
Regional Frameworks	37%	33%	42%	44%	39%	35%
Industry-Specific Frameworks	29%	34%	31%	26%	18%	22%

Note: Data from survey of 183 organizations across 27 countries. Percentages reflect adoption rate within each region. Organizations may adopt multiple frameworks.

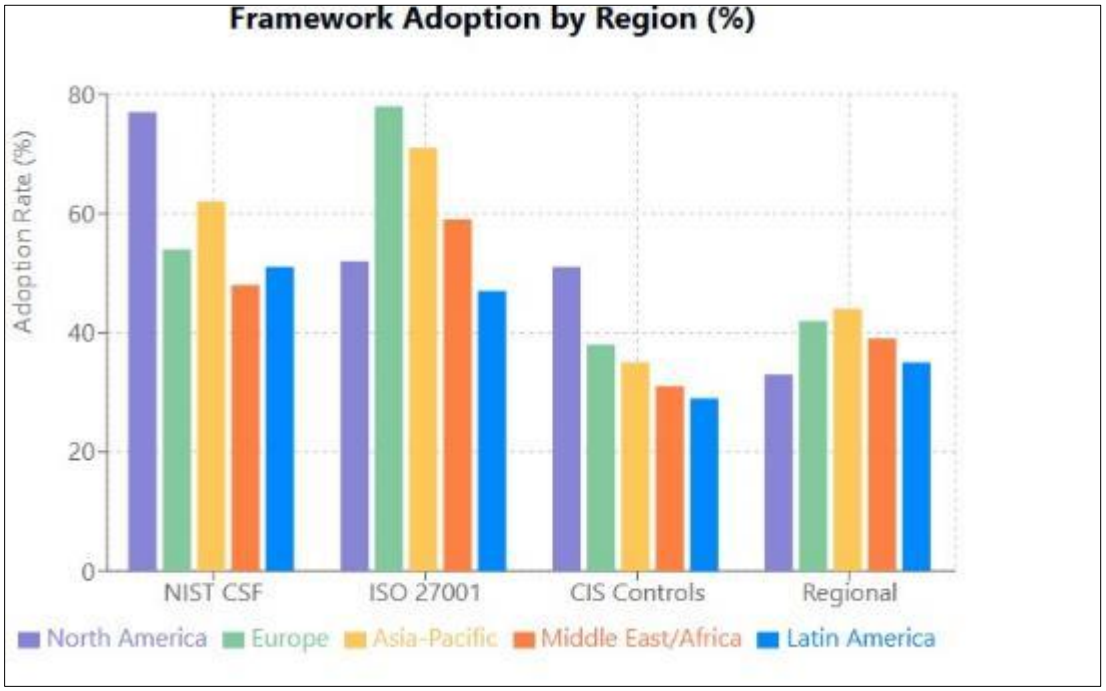

Figure 1 Framework Adaptation by region (%)

4.1.1. Framework Selection Patterns

The most widely adopted frameworks among survey respondents were the NIST Cybersecurity Framework (68%), ISO 27001 (63%), and CIS Controls (42%), with regional variations in adoption patterns. European organizations showed stronger preference for ISO standards (78% adoption rate compared to 52% in North America), while North American organizations demonstrated higher adoption of the NIST CSF (77% compared to 54% in Europe).

Qualitative findings provided context for these selection patterns, revealing that framework choices frequently reflected a combination of industry norms, regulatory alignment, and organizational heritage. As one CISO from a multinational financial institution explained:

"Our framework selection evolved over time based on multiple factors. We started with ISO 27001 because it aligned with other management systems and had global recognition. We later incorporated elements of NIST CSF because it provided more operational guidance and helped us communicate with our U.S. regulators." (Participant 7, Financial Services, Europe)

4.1.2. Adaptation Approaches

Three distinct adaptation approaches emerged from the data: comprehensive implementation, selective adaptation, and hybrid framework development. These approaches were distributed relatively evenly among survey respondents

(comprehensive: 31%, selective: 37%, hybrid: 32%), though with significant variation across organization size categories. Larger organizations (>10,000 employees) were more likely to employ hybrid approaches (48%) compared to small and medium organizations (19%).

Table 2 Framework Adaptation Approaches by Organization Size

Adaptation Approach	Overall	Small (<1,000)	Medium (1,000-10,000)	Large (>10,000)
Comprehensive Implementation	31%	42%	33%	19%
Selective Adaptation	37%	49%	36%	33%
Hybrid Framework Development	32%	9%	31%	48%

Note: Data shows percentage of organizations in each size category utilizing each adaptation approach. Small organizations show preference for simpler approaches, while larger organizations tend toward more complex hybrid models.

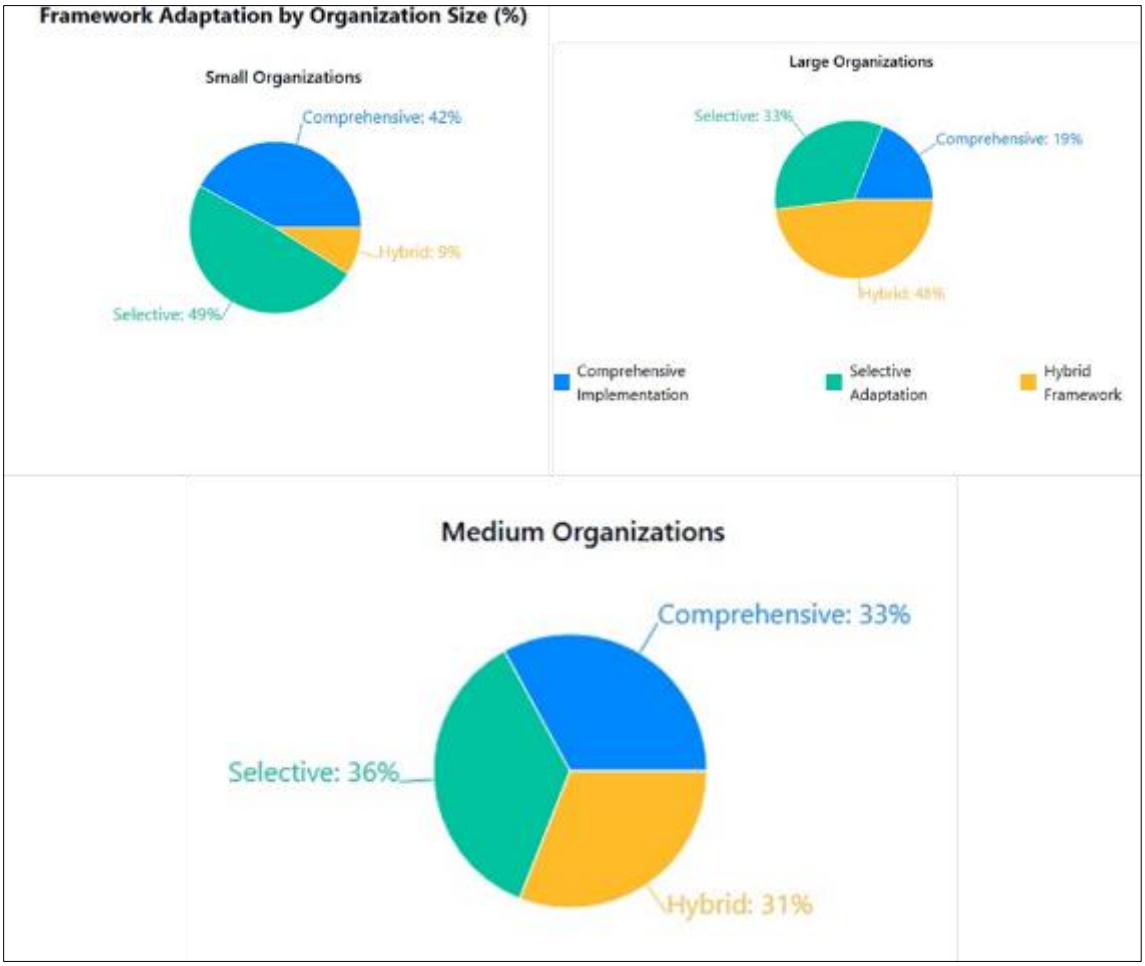

Figure 2 Framework Adaptation by Organization (%)

Comprehensive implementation involved adopting a primary framework with minimal modification, typically maintaining the full control set and assessment methodology. Organizations employing this approach cited benefits including standardization, simplified compliance mapping, and leverage of framework recognition. However, they also reported challenges related to contextual fit and operational friction.

Selective adaptation involved selecting and implementing specific framework components based on perceived relevance to the organization's risk profile and operational context. This approach was particularly common among small and mid-sized organizations with resource constraints, as well as those in specialized industries with unique risk considerations.

A security director from a healthcare organization described their selective approach:

"We recognized that not every control in the frameworks applied equally to our environment. Instead of trying to implement everything, we conducted a methodical analysis of our actual threats and risks, then selected controls that addressed those specific concerns. This focused approach let us allocate our limited resources to controls with the greatest security benefit and least operational disruption." (Participant 18, Healthcare, North America)

Hybrid framework development involved combining elements from multiple frameworks to create customized approaches. Survey data indicated that organizations employing hybrid approaches incorporated elements from an average of 3.4 distinct frameworks. Qualitative findings revealed that hybrid approaches were frequently motivated by needs to:

- Address multiple regulatory requirements simultaneously
- Combine strategic elements from one framework with operational guidance from another
- Leverage industry-specific extensions to general frameworks
- Incorporate emerging risk areas not fully addressed in established frameworks

4.1.3. Integration with Business Operations

A critical dimension of framework implementation involved integration with broader business processes and objectives. Organizations demonstrating higher levels of business integration reported significantly better security-efficiency balance ($r = 0.63$, $p < 0.001$) compared to those implementing frameworks as standalone security initiatives.

Several integration practices emerged as particularly effective:

- Aligning control implementation with business process improvement initiatives
- Mapping security objectives to business outcomes and key performance indicators
- Involving business stakeholders in control selection and implementation planning
- Adapting control implementation based on business context and criticality
- Establishing continuous feedback loops between security and business operations

Quantitative analysis indicated that organizations reporting high levels of business integration were more likely to describe their security programs as "enhancing" rather than "restricting" business operations (74% vs. 23%, $\chi 2 = 38.7$, $p < 0.001$), suggesting that integration contributes to more positive perceptions of security's business value.

4.2. The Role of Emerging Technologies

Emerging technologies played significant roles in enabling more efficient and effective implementation of cyber risk management frameworks. Survey results indicated widespread adoption of various technologies, with particularly strong uptake of security automation (78%), advanced analytics (67%), and integrated risk management platforms (58%).

4.2.1. Technology Implementation Patterns

Analysis revealed three distinct patterns in technology implementation across the sample: technology-led approaches, framework-led approaches, and integrated approaches. These patterns reflected different philosophical perspectives on the relationship between technologies and risk management frameworks.

Technology-led approaches (31% of respondents) prioritized implementation of advanced technological capabilities, with frameworks serving primarily as reference points for coverage assessment. Organizations following this approach emphasized the ability of technologies to address emerging risks more rapidly than framework updates, as well as efficiency gains from automation and analytics.

A technology executive explained this perspective:

"The threat landscape evolves too quickly for frameworks to keep pace. We focus on implementing technologies that provide the capabilities we need, then map those capabilities back to framework requirements as needed for compliance purposes. This keeps us agile and forward-looking rather than constrained by framework boundaries." (Participant 29, Technology Sector, Asia-Pacific)

Framework-led approaches (27% of respondents) positioned frameworks as the primary organizing structure, with technologies selected and implemented specifically to support framework requirements. Organizations adopting this approach emphasized the importance of comprehensive coverage, risk-based prioritization, and alignment with established standards.

Integrated approaches (42% of respondents) represented balanced implementation where frameworks and technologies evolved in tandem, each informing the other. These organizations typically maintained framework alignment while leveraging technologies to enhance implementation efficiency, adaptiveness, and effectiveness.

Integrated approaches correlated most strongly with positive security-efficiency outcomes in quantitative analysis ($r = 0.58$, $p < 0.001$), suggesting benefits from thoughtful integration of technological capabilities within framework structures.

4.2.2. Key Technology Enablers

Several specific technologies emerged as particularly important enablers of balanced risk management approaches:

Security automation technologies, including security orchestration, automation and response (SOAR) platforms and robotic process automation (RPA), demonstrated significant impact on operational efficiency. Organizations implementing comprehensive automation reported average reductions of 31% in time spent on routine security tasks and 47% faster incident response times compared to those with limited automation.

Qualitative insights highlighted the selective application of automation:

"We found the greatest value in automating standardized, repetitive security activities—vulnerability scanning, access reviews, baseline compliance checks. This freed our skilled personnel to focus on complex risk scenarios that require human judgment. The key was identifying the right dividing line between automated and human-driven activities." (Participant 11, Manufacturing, Europe)

Advanced analytics and machine learning applications showed particular value in enhancing risk assessment accuracy and supporting risk-based prioritization. Organizations employing advanced analytics reported increased confidence in risk assessments (mean rating 4.2/5 vs. 3.3/5) and greater precision in resource allocation compared to those using traditional assessment methods.

Integrated risk management platforms that consolidated framework management, control assessment, and reporting functions contributed to both efficiency and effectiveness. Organizations using these platforms reported 43% reductions in time spent on compliance reporting and increased visibility of security status across the organization.

Visualization tools that translated complex risk data into accessible formats improved communication with non-technical stakeholders. Organizations employing advanced visualization reported higher board and executive understanding of cyber risks (mean rating 3.9/5 vs. 2.7/5) compared to those using traditional reporting methods.

4.2.3. Implementation Challenges

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

- Integration difficulties with existing security and IT systems (cited by 73%)
- Skill gaps for effective technology implementation and management (67%)
- Challenges in demonstrating return on investment (61%)
- Maintaining technology alignment with evolving frameworks (58%)
- Managing technology sprawl and redundancy (52%)

Table 3 Technology Implementation Challenges

Challenge	Percentage of Organizations	Small (<1,000)	Medium (1,000-10,000)	Large (>10,000)
Integration difficulties with existing systems	73%	68%	72%	81%
Skill gaps for effective implementation	67%	79%	65%	58%
Challenges demonstrating ROI	61%	74%	63%	49%
Maintaining alignment with evolving frameworks	58%	47%	59%	68%
Managing technology sprawl and redundancy	52%	33%	48%	73%
Data quality and consistency issues	47%	41%	46%	54%
Vendor management complexities	39%	28%	37%	51%

Note: Data shows percentage of organizations reporting each challenge as significant. Different organization sizes face distinct implementation barriers.

Qualitative findings provided context for these challenges, revealing tensions between technology capabilities and organizational readiness. As one participant observed:

"We've learned that successful security technology implementation is only partly about the technology itself. Equally important are the surrounding processes, skills, and governance structures. When we neglected those elements, even the most promising technologies failed to deliver their expected benefits." (Participant 33, Financial Services, Asia-Pacific)

4.2.4. Technology Governance Approaches

Organizations demonstrating successful technology integration typically implemented structured governance approaches for selecting, implementing, and evaluating security technologies. Effective practices included:

- Establishing clear criteria for technology evaluation linked to security and business objectives
- Implementing proof-of-concept processes before full-scale deployment
- Developing skills transformation roadmaps alongside technology implementation
- Creating feedback mechanisms to assess operational impact and security effectiveness
- Maintaining technology inventories and regular rationalization processes

These governance practices correlated with higher reported technology effectiveness ($r = 0.49$, $p < 0.01$) and more favorable security-efficiency outcomes ($r = 0.54$, $p < 0.001$) in the quantitative analysis.

4.3. Governance Structures and Processes

Organizational governance emerged as a critical factor in achieving appropriate security-efficiency balance. Both qualitative and quantitative findings highlighted the importance of well-designed governance structures and processes that facilitate collaboration between security functions and business operations.

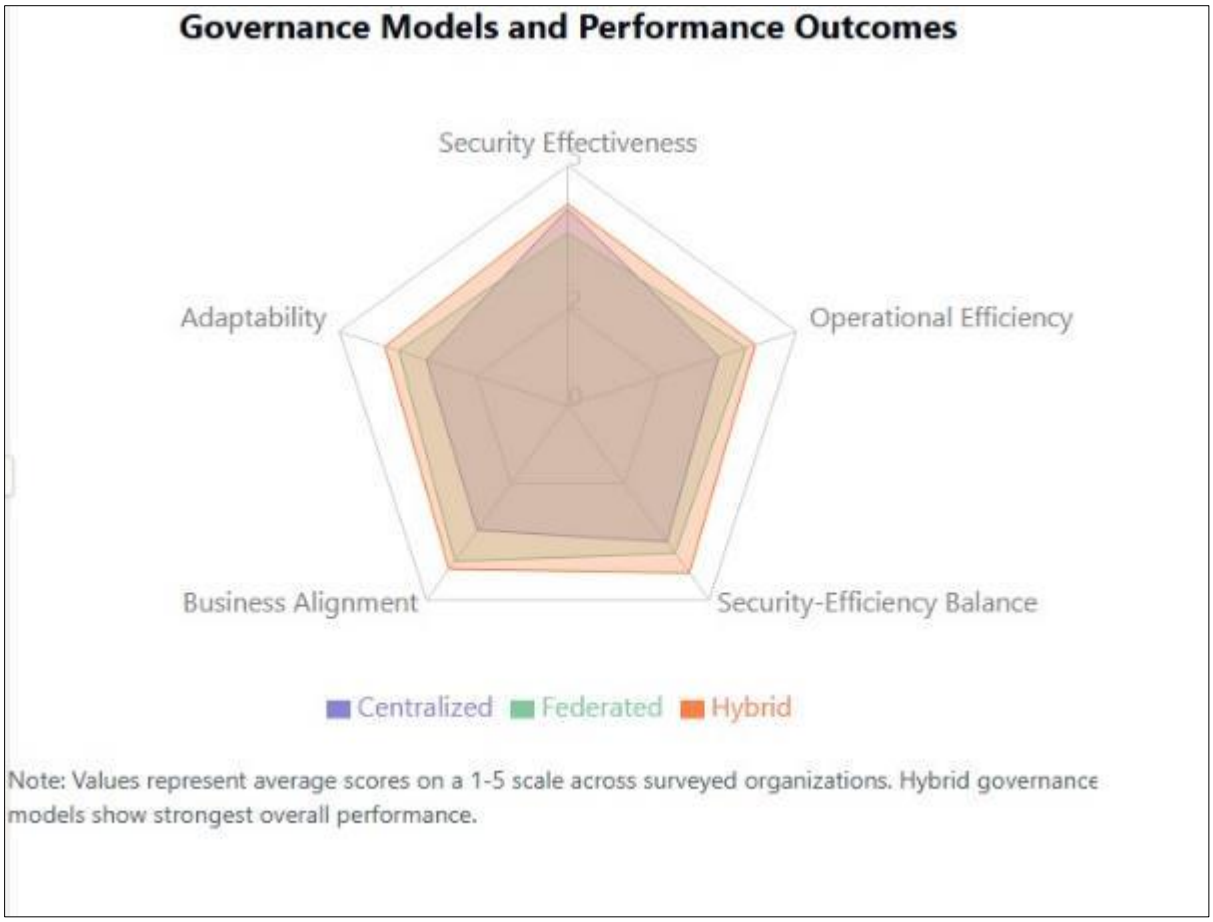

Figure 3 Governance Models and performance outcomes

4.3.1. Governance Models

Three primary governance models were identified across the sample: centralized, federated, and hybrid approaches. The distribution of these models varied significantly by organization size and complexity, with larger and more diverse organizations more frequently employing federated and hybrid models.

Centralized governance models (39% of respondents) positioned security decision-making authority within a single organizational function, typically reporting to the CISO or CIO. These models demonstrated strengths in standardization, clear accountability, and consistent control implementation. However, they often faced challenges related to business alignment and responsiveness to varied operational needs.

Federated governance models (24% of respondents) distributed security responsibilities across business units or functions, with central coordination. These models showed advantages in business alignment and contextual adaptation but sometimes struggled with inconsistent implementation and fragmented oversight.

Table 4 Governance Models and Security-Efficiency Outcomes

Governance Model	Distribution	Security Effectiveness Score (1-5)	Operational Efficiency Score (1-5)	Security-Efficiency Balance Score (1-5)
Centralized	39%	4.1	3.3	3.5
Federated	24%	3.6	3.9	3.8
Hybrid	37%	4.2	4.1	4.3

Note: Data shows distribution of governance models across surveyed organizations and average scores for security effectiveness, operational efficiency, and overall balance. Hybrid models demonstrate strongest overall performance, particularly in achieving security-efficiency balance.

Hybrid governance models (37% of respondents) combined elements of both approaches, typically maintaining centralized authority for framework selection and critical controls while delegating implementation decisions and certain risk acceptance authorities to business units.

Quantitative analysis revealed that hybrid models correlated most strongly with positive security-efficiency outcomes ($r = 0.47$, $p < 0.01$), particularly in complex organizations operating across multiple regions or business lines.

A risk management leader described the evolution toward a hybrid model:

"We transitioned from a purely centralized model because it created too much friction with the business. But a fully federated approach led to inconsistent protection. Our hybrid model maintains central control over our security framework and critical controls, while allowing business units flexibility in implementation approaches and risk decisions within defined parameters. This balance has significantly improved both security effectiveness and business acceptance." (Participant 24, Retail, North America)

4.3.2. Cross-Functional Collaboration Structures

Organizations demonstrating effective security-efficiency balance typically implemented formal structures for cross-functional collaboration. Survey results indicated that the presence of established collaboration mechanisms significantly predicted positive balance outcomes ($\beta = 0.42$, $p < 0.001$) in regression analysis.

Effective collaboration structures included:

- Security champions programs embedded within business units (implemented by 67% of high-performing organizations)
- Cross-functional working groups for security initiatives (78%)
- Formal business representation in security governance committees (81%)
- Joint risk assessment processes involving both security and business stakeholders (72%)
- Collaborative control design workshops (64%)

These structures provided mechanisms for ongoing dialogue between security and business functions, facilitating better understanding of both security requirements and operational constraints.

4.3.3. Risk Acceptance and Exception Processes

Formalized processes for risk acceptance and control exceptions emerged as particularly important governance mechanisms. Organizations with well-defined exception processes reported significantly better security-efficiency balance (mean rating 4.1/5 vs. 2.8/5) compared to those with ad hoc approaches.

Effective exception processes shared several characteristics:

- Clear criteria for acceptable exceptions based on risk assessment
- Defined approval authorities appropriate to risk levels
- Temporary exception periods with required reassessment
- Documentation requirements including business justification
- Alternative control options for risk mitigation

A security executive described their approach:

"We recognized that no security framework fits perfectly in every situation. Rather than forcing compliance that might seriously impair business functions, we developed a structured exception process that ensures risks are properly assessed, appropriately approved, and regularly reviewed. This transformed security exceptions from hidden shadows to managed risks." (Participant 4, Energy, Middle East)

4.3.4. Metric Development and Performance Measurement

The development and application of balanced metrics emerged as a critical governance function. Organizations employing metrics that addressed both security effectiveness and operational efficiency reported better overall outcomes than those focusing predominantly on either security or efficiency measures.

Effective measurement approaches typically included:

- Security effectiveness metrics (e.g., vulnerability remediation rates, detection coverage)
- Operational impact metrics (e.g., user experience measures, process cycle times)
- Balanced scorecards combining security and business perspectives
- Outcome-oriented rather than activity-oriented measures
- Regular review and refinement of metric relevance

Quantitative analysis revealed that organizations with balanced measurement approaches were significantly more likely to report having achieved appropriate security-efficiency equilibrium (odds ratio = 3.8, $p < 0.001$) compared to those with imbalanced approaches.

4.4. Global Harmonization Challenges and Approaches

Organizations operating across multiple geographic regions faced particular challenges in implementing consistent cyber risk management approaches while addressing regional variations. Survey results indicated that 78% of multinational respondents considered regional harmonization a significant challenge, with regulatory fragmentation identified as the primary obstacle (cited by 83%).

4.4.1. Sources of Regional Variation

Analysis identified four primary sources of regional variation that complicated harmonized risk management:

Regulatory requirements varied significantly across jurisdictions, with particular divergence noted between European, North American, and Asian regulatory approaches. Survey respondents reported managing an average of 7.3 distinct cybersecurity regulatory frameworks (range: 1-23), creating substantial compliance complexity.

Organizational maturity levels often varied across regions within the same company, reflecting different historical investments, growth patterns, and acquisition histories. These variations complicated consistent implementation of frameworks and controls.

Infrastructure and technology environments differed across regions, influenced by factors including local market conditions, legacy systems, and technology availability. These differences affected both risk profiles and control implementation approaches.

Cultural approaches to security and risk showed regional variation, influencing factors such as policy adherence, risk acceptance, and security awareness. Organizations reported challenges in developing security approaches that remained effective across different cultural contexts.

4.4.2. Harmonization Strategies

Organizations employed several strategies to address these variations while maintaining appropriate global consistency. The most effective approaches combined elements of standardization with controlled flexibility:

Core-and-flex frameworks established mandatory global controls ("core") while allowing regional adaptation for specific requirements ("flex"). Organizations employing this approach typically identified 60-70% of controls as core requirements, with remaining elements subject to regional adaptation.

A global security director explained:

"We developed a tiered model with three categories: global mandatory controls that are non-negotiable, recommended controls with implementation flexibility, and region-specific controls addressing local requirements. This structure maintains consistency where it matters most while accommodating legitimate regional differences." (Participant 16, Financial Services, Global)

Control mapping and translation layers enabled organizations to maintain consistent internal control frameworks while demonstrating compliance with varied regional requirements. These approaches typically involved developing comprehensive control ontologies with mapped relationships to regional frameworks and regulations.

Principle-based rather than prescriptive approaches focused on desired security outcomes rather than specific implementation methods. This allowed regional operations to achieve security objectives through methods appropriate to their contexts while maintaining consistent security postures.

Federated governance with global oversight balanced local decision-making with enterprise consistency. These models typically maintained global authority for framework definition and critical risk decisions while delegating implementation authority to regional security functions.

4.4.3. Technology Enablers for Harmonization

Technology solutions played important roles in enabling harmonized approaches across regions. Particularly valuable technologies included:

- Integrated compliance management platforms supporting multiple framework mappings (used by 67% of multinational respondents)
- Centralized policy management systems with regional customization capabilities (58%)
- Automated compliance verification tools reducing manual assessment burden (53%)
- Analytics solutions providing cross-regional visibility and comparison (47%)
- Translation management for security policies and training materials (41%)

Organizations leveraging these technologies reported greater confidence in their global security posture (mean rating 3.9/5 vs. 2.7/5) compared to those with limited technology support for harmonization.

4.4.4. Harmonization Maturity Model

Based on the research findings, we developed a four-level maturity model for global harmonization of cyber risk management approaches:

- **Level 1: Fragmented** - Regions operate independently with minimal coordination, using different frameworks and standards with limited visibility across regions. This approach creates significant inconsistency, compliance gaps, and inefficient resource utilization.
- **Level 2: Coordinated** - Central coordination mechanisms exist with shared frameworks, but implementation remains largely independent by region. Information sharing increases, but substantial variations persist in control implementation and effectiveness.
- **Level 3: Standardized** - Global framework and core controls are consistently implemented across regions, with controlled regional variations for specific requirements. Governance mechanisms ensure appropriate exceptions and adaptations.
- **Level 4: Integrated** - Fully harmonized approach with dynamic adaptation to both global and regional requirements. Sophisticated technology enablement provides comprehensive visibility, automated compliance verification, and continuous monitoring across all regions.

Table 5 Global Harmonization Maturity Levels

Maturity Level	Description	Distribution	Risk Management Effectiveness (1-5)	Compliance Efficiency (1-5)
Level 1: Fragmented	Regions operate independently with minimal coordination	13%	2.3	2.1
Level 2: Coordinated	Central coordination with shared frameworks but independent implementation	48%	3.4	3.1
Level 3: Standardized	Global framework with core controls and controlled regional variations	31%	4.2	3.9
Level 4: Integrated	Fully harmonized approach with dynamic adaptation	8%	4.6	4.5

Note: Data shows distribution of multinational organizations across harmonization maturity levels and average scores for global risk management effectiveness and compliance efficiency. Higher maturity levels correlate with improved outcomes in both dimensions.

Survey results indicated that most multinational organizations operated at Level 2 (48%) or Level 3 (31%), with only 8% achieving Level 4 integration. Organizations at higher maturity levels reported significantly better global risk management effectiveness ($F(3,72) = 18.6$, $p < 0.001$) and more efficient compliance approaches ($F(3,72) = 14.3$, $p < 0.001$) compared to those at lower levels.

4.5. The Adaptive Security-Efficiency Model

Building on the research findings, we developed an "Adaptive Security-Efficiency Model" to provide organizations with a structured approach for achieving appropriate balance between security controls and operational requirements. This model integrates insights regarding framework adaptation, technology enablement, governance approaches, and harmonization strategies.

4.5.1. Model Components

The Adaptive Security-Efficiency Model comprises four interconnected components, each addressing a critical dimension of balanced risk management:

Integrated Risk Governance establishes the organizational structures and processes for aligning security objectives with business imperatives. This component encompasses:

- Cross-functional governance bodies with appropriate business representation
- Formalized risk acceptance and exception processes
- Balanced performance metrics addressing both security and efficiency
- Collaborative decision-making protocols for security investments and controls

Contextual Framework Adaptation provides approaches for adapting voluntary standards to organizational contexts while maintaining their essential benefits. This component includes:

- Framework selection based on organizational requirements and industry context
- Control prioritization methods balancing risk reduction with operational impact
- Hybrid framework development leveraging multiple standards where appropriate
- Control implementation approaches aligned with business processes and workflows

Strategic Technology Integration addresses the selection and implementation of technologies that enhance both security effectiveness and operational efficiency. This component covers:

- Technology selection criteria aligned with security and business objectives
- Automation strategy identifying appropriate processes for technology enablement
- Analytics capabilities supporting risk-based decision-making
- Implementation approaches that address organizational readiness and skill requirements

Dynamic Adaptation Mechanisms enable ongoing evolution of the security approach in response to changing threats, technologies, and business requirements. This component encompasses:

- Feedback loops gathering operational impact information
- Control effectiveness measurement and refinement processes
- Continuous improvement methodologies for security processes
- Threat intelligence integration for proactive adaptation

4.5.2. Implementation Approach

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

- **Phase 1: Assessment and Alignment** involves evaluating current security approaches, business objectives, and efficiency challenges to establish a baseline and define target outcomes. This phase includes stakeholder engagement to build shared understanding of security-efficiency goals.
- **Phase 2: Foundation Development** focuses on establishing core governance structures, selecting and adapting appropriate frameworks, and implementing foundational technologies. This phase creates the essential infrastructure for balanced risk management.

- **Phase 3: Integration and Optimization** addresses deeper integration of security with business processes, optimization of controls for efficiency, and enhanced technology enablement. This phase significantly improves both security effectiveness and operational efficiency.
- **Phase 4: Continuous Evolution** establishes mechanisms for ongoing adaptation to evolving threats, technologies, and business requirements. This phase ensures long-term sustainability of appropriate security-efficiency balance.

4.5.3. Validation and Application

The model was validated through expert review with 16 cybersecurity leaders and pilot application in five organizations across different sectors. Initial results indicate that the model 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 after initial implementation.

The model was particularly effective in helping organizations:

- Identify and address governance gaps inhibiting effective balance
- Develop more contextually appropriate framework adaptations
- Select and implement appropriate enabling technologies
- Establish effective feedback mechanisms for continuous improvement

5. Discussion

5.1. The Evolution of Security-Efficiency Paradigms

Our findings reveal an ongoing evolution in how organizations conceptualize the relationship between security and operational efficiency. Traditional approaches often positioned security and efficiency as inherently opposing forces, creating an implicit assumption that strengthening security necessarily reduced operational agility and efficiency. This paradigm frequently led to security being viewed as a business constraint rather than an enabler.

The research indicates a shift toward more integrated perspectives, where security and efficiency are increasingly viewed as complementary rather than contradictory objectives. Organizations demonstrating this evolved perspective share several characteristics:

- They design security controls with operational context in mind, seeking to enhance rather than impede critical business processes
- They involve business stakeholders in security decision-making, ensuring operational considerations inform control selection and implementation
- They leverage technologies that simultaneously improve security effectiveness and operational efficiency
- They implement feedback mechanisms that rapidly identify and address unintended operational impacts

This paradigm shift aligns with broader trends in cybersecurity toward more business-aligned, risk-based approaches. As one participant observed:

"We've moved away from the mentality that security should be maximized regardless of business impact. We now recognize that excessive security friction ultimately undermines security itself, as users find workarounds or operations become untenable. Our goal is effective security that enables rather than constrains the business." (Participant 9, Retail, North America)

This evolution represents an important maturation of the cybersecurity function, moving from a primarily technical orientation toward a more strategic business role. Organizations furthest in this evolution demonstrated security functions that actively contributed to business objectives beyond risk reduction, including customer trust, operational efficiency, and market differentiation.

5.2. Voluntary Standards as Flexible Foundations

The research highlights the critical role of voluntary cybersecurity standards in providing structured approaches to risk management while allowing appropriate adaptation to organizational contexts. Rather than viewing frameworks as

rigid requirements, successful organizations treated them as flexible foundations that could be tailored to their specific needs.

This finding challenges both the strict compliance-oriented application of frameworks and the entirely ad hoc approaches to security. The most effective organizations maintained the structural benefits of established frameworks—comprehensiveness, common terminology, continuous improvement cycles—while adapting specific elements to their operational realities.

The emergence of hybrid approaches combining elements from multiple frameworks reflects increasing organizational sophistication in framework utilization. Rather than selecting a single framework based on regional prevalence or industry norms, organizations thoughtfully selected complementary elements that addressed their specific risk profiles and operational requirements.

This approach aligns with arguments from standards development bodies themselves, which increasingly emphasize the adaptable nature of their frameworks. For example, NIST explicitly describes the Cybersecurity Framework as "a risk-based approach to managing cybersecurity risk that is composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. Each Framework component reinforces the connection between business drivers and cybersecurity activities" (NIST, 2018, p. 4).

5.3. The Transformative Potential of Emerging Technologies

Our findings demonstrate the significant potential of emerging technologies to transform cyber risk management, potentially resolving longstanding tensions between security rigor and operational efficiency. The most impactful technologies enable organizations to achieve both enhanced security and improved operational experience—addressing the security-efficiency dilemma directly rather than requiring tradeoffs.

For example, security automation technologies demonstrated particular value in reducing manual effort while improving consistency of control implementation. Advanced analytics enhanced risk visibility without creating additional assessment burden. And integrated platforms streamlined compliance activities while providing better insights into security posture.

However, the research also revealed important cautions regarding technology implementation. Technology adoption without appropriate governance, skills development, and process integration often failed to deliver expected benefits and sometimes created new problems. As one participant noted:

"We've learned that technology alone doesn't solve the security-efficiency challenge. In fact, poorly implemented security technology can make things worse—adding complexity without corresponding benefits. Successful implementation requires thoughtful alignment with business processes, appropriate skill development, and ongoing measurement of actual outcomes." (Participant 21, Technology, North America)

This finding aligns with broader research on digital transformation, which consistently demonstrates that technology adoption must be accompanied by organizational and process changes to deliver meaningful benefits (Vial, 2019).

5.4. Governance as the Essential Foundation

A consistent theme across our findings is the central importance of well-designed governance structures and processes in achieving appropriate security-efficiency balance. Effective governance provides the foundation for everything else—framework adaptation, technology implementation, and regional harmonization all depend on governance mechanisms that align security objectives with business imperatives.

The research identified several critical governance capabilities that distinguished organizations achieving optimal balance:

- **Multi-stakeholder decision structures** that incorporated both security and business perspectives in risk management decisions
- **Formalized exception processes** that provided controlled flexibility where standard controls created excessive operational burden
- **Balanced measurement systems** that tracked both security effectiveness and operational impact
- **Clear accountability models** that assigned appropriate responsibility for both security implementation and business risk acceptance

These governance capabilities enabled organizations to make more nuanced decisions about security-efficiency tradeoffs, avoiding both under-protection and over-control. They created structured mechanisms for dialogue between security and business functions, facilitating better mutual understanding and more integrated approaches.

This finding confirms and extends previous research by Ibrahim and Kant (2020) and Talaoui and Kohtamäki (2022) on the importance of governance in security-efficiency balance, while providing more detailed insight into specific governance mechanisms that prove most effective.

5.5. The Global Harmonization Challenge

Our research reveals significant ongoing challenges in harmonizing cyber risk management approaches across global operations. Despite the existence of international standards and frameworks, substantial regional variations persist in regulatory requirements, cultural approaches to risk, and implementation capabilities.

These variations create particular difficulties for multinational organizations seeking to implement consistent security approaches while addressing local requirements. The research demonstrates that neither completely standardized global approaches nor entirely localized approaches prove optimal in most cases. Instead, successful organizations implement thoughtfully designed core-and-flex models that maintain consistency in critical areas while allowing appropriate regional adaptation.

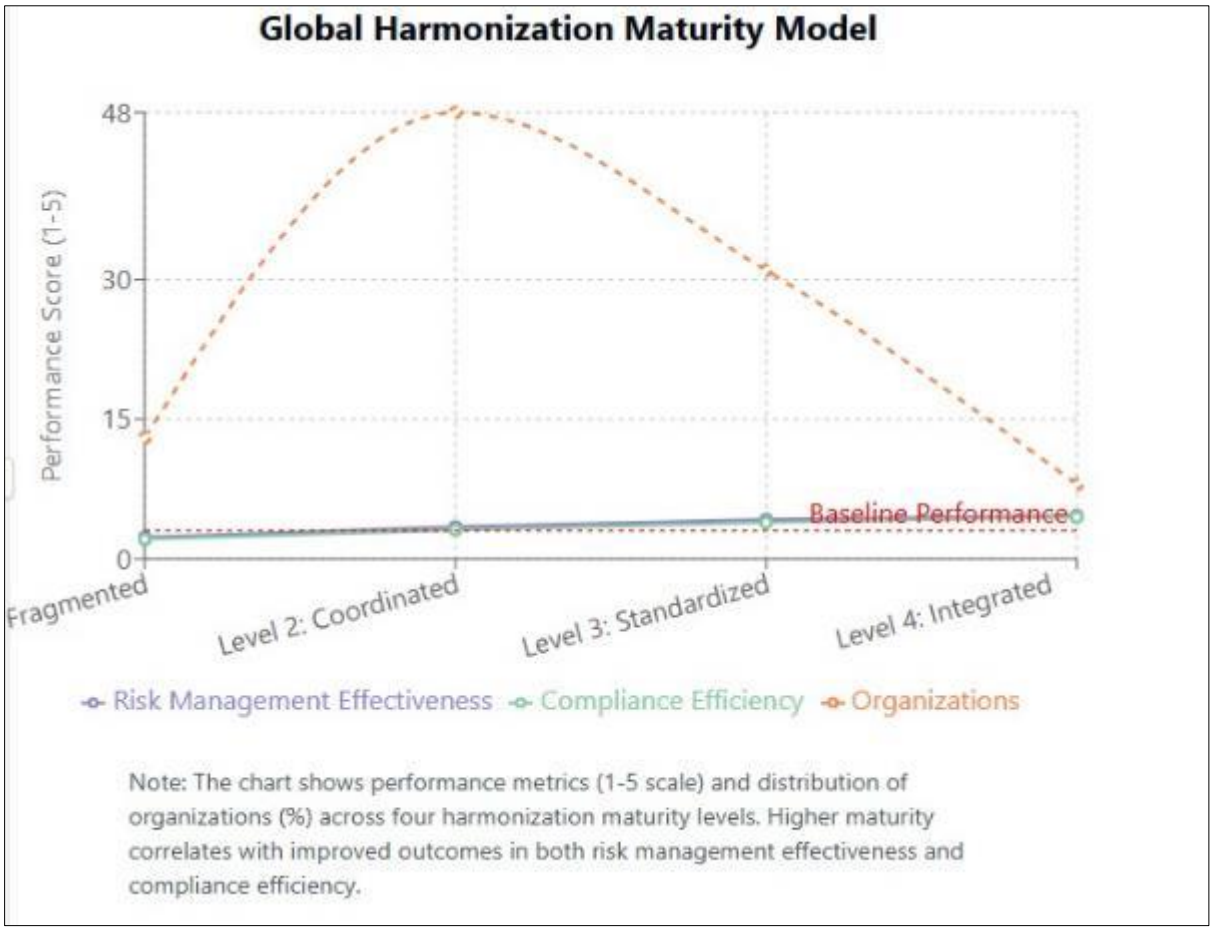

Figure 4 Global Harmonization Maturity Model

This finding has important implications for both organizational practice and policy development. For organizations, it suggests the need for more sophisticated approaches to global security governance that balance centralized and distributed authorities appropriately. For policymakers and standards bodies, it highlights the importance of developing frameworks with inherent flexibility and clear distinctions between foundational requirements and implementation details.

The harmonization maturity model proposed in this research offers a potential path forward, providing organizations with a structured progression toward more integrated global approaches. By focusing first on governance alignment and core control standardization before attempting full integration, organizations can develop more sustainable approaches to global harmonization.

5.6. Implications for Practice

Our findings have several important implications for cybersecurity practitioners and organizational leaders:

- **Security leaders** should prioritize the development of cross-functional governance structures that facilitate meaningful business input into security decision-making. These structures create the foundation for balanced approaches that address both risk management and operational needs.
- **Risk management teams** should approach framework implementation with a focus on contextual adaptation rather than rigid compliance. This involves thoughtful selection of frameworks based on organizational needs, appropriate tailoring of controls, and development of hybrid approaches where beneficial.
- **Technology executives** should evaluate security technologies not only for their risk reduction capabilities but also for their potential operational benefits or burdens. Technologies that simultaneously enhance security and efficiency offer particularly compelling value propositions.
- **Business leaders** should engage proactively with security initiatives rather than viewing them as technical impositions. Early business involvement in control design and implementation planning can significantly reduce downstream friction and improve security effectiveness.
- **Global organizations** should develop structured approaches to regional variation, clearly distinguishing between controls requiring global consistency and those allowing regional adaptation. Developing these models proactively prevents both security inconsistency and unnecessary operational disruption.

The Adaptive Security-Efficiency Model proposed in this research offers organizations a structured approach for implementing these recommendations, providing practical guidance for achieving appropriate balance within their specific contexts.

5.7. Limitations and Future Research

This study has several limitations that suggest directions for future research. First, while the sample included organizations across multiple regions and sectors, it predominantly represented larger organizations with established security programs. Future research should examine security-efficiency balance in smaller organizations and those with less mature security functions.

Second, the study provides a snapshot of current practices but offers limited insight into how security-efficiency balance evolves over time within organizations. Longitudinal studies tracking organizations through their maturation journey would provide valuable additional perspectives.

Third, while the research identified the importance of cultural factors in security implementation, it did not deeply explore how cultural variations influence security-efficiency perceptions and approaches. More focused examination of cultural dimensions would enhance understanding of these dynamics.

Several specific areas warrant further investigation:

- Development and validation of quantitative metrics for evaluating security-efficiency balance
- Examination of how emerging technologies, particularly artificial intelligence, affect security-efficiency dynamics over longer time horizons
- Investigation of security-efficiency considerations in specific high-risk domains such as critical infrastructure and healthcare
- Analysis of how regulatory approaches influence organizational ability to achieve appropriate security-efficiency balance

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 increasingly complex digital environments.

6. Conclusion

This research investigated how 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 from organizations across 27 countries, we examined framework adaptation approaches, technology implementation patterns, governance structures, and global harmonization challenges.

The findings demonstrate that achieving appropriate security-efficiency balance requires a multifaceted approach addressing governance, framework adaptation, technology integration, and adaptation mechanisms. Organizations that successfully navigate this balance demonstrate three key characteristics: integrated risk governance structures incorporating both security and business perspectives; dynamic adaptation of voluntary frameworks to organizational contexts; and strategic implementation of technologies that enhance both security effectiveness and operational efficiency.

The research revealed significant variation in how organizations adapt voluntary frameworks, with approaches ranging from comprehensive implementation to selective adaptation to hybrid development combining elements from multiple frameworks. Each approach offers distinct advantages and challenges, with hybrid approaches demonstrating particular effectiveness in complex organizations managing multiple requirements.

Emerging technologies play increasingly important roles in enabling balanced risk management, with security automation, advanced analytics, and integrated platforms offering capabilities that potentially resolve traditional tensions between security rigor and operational agility. However, successful technology implementation requires appropriate governance, skills development, and process integration to deliver meaningful benefits.

For organizations operating globally, harmonizing risk management approaches across regions presents particular challenges stemming from regulatory fragmentation, organizational maturity disparities, and varied cultural approaches to risk. Successful organizations address these challenges through sophisticated governance models that balance global consistency with controlled regional adaptation.

Based on these findings, we developed an Adaptive Security-Efficiency Model that provides organizations with a structured approach for achieving appropriate balance between security controls and operational requirements. This model integrates insights regarding governance, framework adaptation, technology enablement, and adaptation mechanisms into a comprehensive framework for balanced risk management.

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 an increasingly complex global environment.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., Moore, T., & Savage, S. (2021). Measuring the cost of cybercrime. In The economics of information security and privacy (pp. 265-300). Springer.

[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] 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

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

[7] Center for Internet Security (CIS). (2021). CIS Controls v8. Retrieved from https://www.cisecurity.org/controls/

[8] 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

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

[10] Dykstra, J., & Spafford, E. H. (2018). The case for disappearing cyber security. Communications of the ACM, 61(7), 40-42.

[11] Georgiadou, A., Mouzakitis, S., & Askounis, D. (2022). Assessing MENA countries' readiness for cybersecurity integration in digital transformation initiatives. Digital Policy, Regulation and Governance, 24(1), 47-64.

[12] 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.

[13] Hsu, C., Wang, T., & Lu, A. (2021). The impact of ISO 27001 certification on firm performance. IT Professional, 23(1), 27-34.

[14] Ibrahim, A., & Kant, S. (2020). Analyzing the tradeoff between security and performance in IoT systems. 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 1832-1839.

[15] ISO/IEC. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. International Organization for Standardization.

[16] Jalali, M. S., Kaiser, J. P., Siegel, M., & Madnick, S. (2020). The internet of things promises new benefits and risks: A systematic analysis of adoption dynamics of IoT products. IEEE Security & Privacy, 17(2), 39-48.

[17] Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80(5), 973-993.

[18] Kolini, F., & Janczewski, L. (2022). Decision-making factors in cybersecurity investment: A systematic literature review. Information & Computer Security, 30(5), 609-629.

[19] Kuner, C., Cate, F. H., Millard, C., Svantesson, D. J. B., & Lynskey, O. (2017). Risk management in data protection. International Data Privacy Law, 7(2), 95-98.

[20] Kunnathur, A. (2015). Information security in supply chains: A management control perspective. Information & Computer Security, 23(5), 476-496.

[21] Libertini, G., Marlin, S., Wallace, G., & Yan, D. (2021). Designing cybersecurity into products. The Computer Journal, 64(5), 641-652.

[22] Mahdavifar, S., Ghorbani, A. A., Khezri, M. R., & Omidvar, R. (2021). Machine learning for Internet of Things security: A comprehensive survey. IEEE Internet of Things Journal, 8(18), 14572-14599.

[23] Mariani, A., Nicoletti, L., &Ghidini, G. (2022). Balancing cybersecurity with production efficiency: Trade-offs and sustainable approaches for managing cybersecurity in Industry 4.0. Computers in Industry, 134, 103564.

[24] Morris, D. K., Vandeventer, J., & Linder, A. (2021). Balancing cybersecurity with business requirements: A financial services industry study. Information & Computer Security, 29(5), 729-753.

[25] Mwenya, M., & Ali, M. (2019). An exploration of organisations' approaches to implementing the NIST cybersecurity framework. In CONF-IRM 2019 Proceedings. AIS Electronic Library.

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

[27] Pham, D. H., Yeo, Z., Prabhu, B., & Ang, S. K. (2022). Cybersecurity implementations in manufacturing enterprises: A systematic literature review. Computers & Security, 113, 102539.

[28] Ramirez, A., & Kibel, M. (2020). The evolution of cybersecurity frameworks: From compliance to active defense. IT Professional, 22(5), 47-52.

[29] Rodríguez-Vidal, M., Janicke, H., Jones, K., & Marklund, J. (2023). The evolving landscape of global cybersecurity frameworks: A comparative analysis. Information & Computer Security, 31(1), 105-127.

[30] Romano, A., Bongiovanni, I., & Schiliro, F. (2022). Automation in cybersecurity: State of the art and open issues. Computers & Security, 112, 102514.

[31] Shafiq, M., Tian, Z., Bashir, A. K., Jolfaei, A., & Yu, X. (2021). Data mining and machine learning methods for cyber security intrusion detection: A survey. IEEE Communications Surveys & Tutorials, 24(1), 1-26.

[32] Shaw, R., Atkins, A., Bower, D. A., & Black, S. (2020). Critical factors for the successful automation of cybersecurity processes. IEEE Access, 8, 145384-145410.

[33] Simonet, D., & Green, M. (2021). Information security framework fusion: The case of multinational corporations. Journal of Global Information Management, 29(5), 1-19.

[34] Talaoui, Y., &Kohtamäki, M. (2022). Cybersecurity investment and organizational performance: A resource management perspective. Business Process Management Journal, 28(1), 300-320.

[35] van der Kleij, R., Schraagen, J. M., Werkhoven, P., & De Dreu, C. K. (2017). How conversations change over time in face-to-face and video-mediated communication. Small Group Research, 48(2), 123-146.

[36] Vejačka, M., &Štofa, T. (2021). Implementation of cybersecurity management framework standards in European and Asian businesses. Digital Policy, Regulation and Governance, 23(6), 578-595.

[37] Vial, G. (2019). Understanding digital transformation: A review and a research agenda. The Journal of Strategic Information Systems, 28(2), 118-144.

[38] von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97-102.

[39] Zheng, J., Cai, Z., Yu, J., Wang, X., & Yang, Y. (2021). Dynamic resource allocation for cybersecurity analytics using deep reinforcement learning. IEEE Internet of Things Journal, 8(9), 7205-7219.