ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768844
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

Developing an Integrated Framework for Cybersecurity and Enterprise Risk Management to Enhance Organizational Resilience

Imrana Alfa Dahir[1] Aliyu Buba Dahiru [2]

[1,2]Computer Engineering Department, Federal Polytechnic Mubi, Adamawa State, Nigeria

07037770897 and 080-81433412 **EMAIL**: imrana902001@yahoo.co.uk

tetfund
TERTIARY EDUCATION TRUST FUND

Abstract

The increasing frequency and sophistication of cyber threats have elevated cybersecurity from a technical concern to a strategic organizational priority. At the same time, organizations are operating in increasingly complex and uncertain environments characterized by technological disruptions, regulatory pressures, and evolving risk landscapes. While Enterprise Risk Management (ERM) provides a structured approach for identifying and managing organizational risks, cybersecurity is often managed separately, resulting in fragmented risk governance and reduced organizational resilience. This study develops an integrated framework that aligns cybersecurity and enterprise risk management practices to enhance organizational resilience in the face of emerging cyber threats and business uncertainties. The study adopts a qualitative conceptual research approach based on a comprehensive review of scholarly literature, industry reports, international standards, and established cybersecurity and risk management frameworks published between 2020 and 2026. Drawing on Resilience Theory, Socio-Technical Systems Theory, and Enterprise Risk Management principles, the proposed framework integrates governance, cyber risk assessment, cybersecurity controls, incident response, business continuity planning, and continuous monitoring within a unified risk management structure. The study argues that effective integration of cybersecurity and ERM enables organizations to improve risk visibility, strengthen decision-making, enhance cyber resilience, and support business continuity. The proposed framework provides both theoretical and practical contributions by offering a holistic approach to managing cyber risks while promoting long-term organizational resilience in an increasingly digital and interconnected environment.

Keywords: Cybersecurity; Enterprise Risk Management; Organizational Resilience; Cyber Risk Governance; Cyber Resilience; Risk Management; Digital Security

1. Introduction

The accelerating digitization of business operations has made cybersecurity a board-level issue rather than a purely technical concern. As organizations expand their use of

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768844
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

cloud services, interconnected platforms, digital workflows, and data-driven decision-making, the consequences of cyber incidents have become broader and more severe, affecting operations, reputation, compliance, and strategic continuity. Recent evidence shows that the economic impact of cyber incidents remains substantial, with IBM reporting that the average global cost of a data breach in 2024 reached USD 4.88 million, while financial-sector breaches averaged USD 6.08 million, underscoring the disproportionate exposure of organizations that handle sensitive and high-value data. At the same time, the World Economic Forum's Global Cybersecurity Outlook 2025 highlights persistent resilience gaps and workforce shortages, indicating that many organizations still struggle to match rising threat complexity with adequate capability and preparedness.

In response to this environment, cybersecurity can no longer be managed in isolation from broader organizational risk processes. Enterprise Risk Management provides the structures through which organizations identify, assess, prioritize, and monitor risks across strategic, operational, financial, and compliance domains, but in practice cyber risk is often treated as a separate technical silo. This fragmentation weakens risk visibility and can produce inconsistent decisions about investment, governance, and response. NIST's revised guidance on integrating cybersecurity and enterprise risk management emphasizes that directors and senior leaders must understand cybersecurity posture as part of enterprise risk oversight, and that cybersecurity risk decisions should align with strategic objectives. The updated NIST Cybersecurity Framework (CSF) 2.0 also frames cybersecurity as a governance and risk communication issue, designed to help organizations of any size or maturity better understand, prioritize, and communicate cybersecurity efforts in line with mission and regulatory expectations.

The need for integration is especially urgent because cyber risk has become entangled with other enterprise risks, including supply-chain disruption, privacy exposure, regulatory non-compliance, operational downtime, and reputational damage. NIST CSF 2.0 explicitly links cybersecurity outcomes to governance, risk management, supply-chain risk management, incident response, and recovery, reinforcing the view that cyber resilience depends on enterprise-wide coordination rather than isolated controls. Recent research also suggests that integrating cyber risk into ERM improves performance by strengthening cross-functional decision-making and enabling a more coherent approach to risk treatment. From this perspective, an integrated framework is not simply an administrative convenience; it is a governance requirement for organizations seeking to sustain resilience in an environment where digital interdependence increases both the frequency and the cascading effects of cyber incidents.

Organizational resilience has therefore become a central concern in cybersecurity scholarship and practice. Resilient organizations are not only able to withstand disruption but also to absorb shocks, recover critical functions, and adapt their structures and controls to emerging threats. This requires a continuous cycle of risk identification, control selection, incident response, recovery planning, and strategic learning. The challenge is that many organizations possess some of these elements in separate programs, yet lack a unifying framework that connects cybersecurity controls with enterprise risk appetite, governance priorities, and business continuity goals. The

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768844
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

result is often duplicated effort in some areas and blind spots in others. A more integrated approach can help organizations align technical defenses with managerial oversight, ensuring that cybersecurity investment is guided by risk significance rather than by fragmented departmental priorities.

This study responds to that gap by developing an integrated framework that brings cybersecurity and Enterprise Risk Management into a single organizational resilience architecture. The framework is intended to connect governance, cyber risk assessment, cybersecurity controls, incident response, business continuity planning, and continuous monitoring in a way that supports enterprise-wide accountability and adaptive decision-making. It builds on contemporary risk-management guidance, including NIST's integration model and the broader principle that risk practices should be proportionate to organizational mission, tolerance, and context. By treating cybersecurity as one component of a wider risk portfolio, the framework aims to improve risk visibility, support prioritization, and strengthen resilience against both direct cyber threats and the wider business disruptions that often follow them.

The contribution of the paper is both conceptual and practical. Conceptually, it positions cybersecurity and ERM as complementary disciplines rather than competing functions, and uses this integration to explain how resilience is produced through coordinated governance and risk treatment. Practically, it offers organizations a structured pathway for embedding cyber risk into enterprise decision-making, especially where board oversight, regulatory scrutiny, and stakeholder expectations demand clearer accountability. In an environment where resilience shortfalls remain common and cyber incidents continue to impose high financial and operational costs, an integrated framework provides a defensible basis for improving preparedness, response, and recovery while supporting long-term organizational stability.

2. Literature Review

The rapid digital transformation of organizations has elevated cybersecurity from a technical function to a strategic organizational priority. As organizations increasingly rely on cloud computing, artificial intelligence (AI), the Internet of Things (IoT), digital platforms, and interconnected information systems, the frequency, sophistication, and business impact of cyber threats have grown considerably. Cybersecurity is therefore no longer viewed solely as the protection of information systems but as an essential component of corporate governance, organizational resilience, and enterprise performance (World Economic Forum, 2025; NIST, 2024). Modern organizations are expected to integrate cybersecurity into strategic planning to protect digital assets, maintain business continuity, preserve stakeholder confidence, and comply with evolving regulatory requirements.

The contemporary cyber threat landscape has become increasingly complex. Organizations are exposed to ransomware, phishing, insider threats, advanced persistent threats, supply-chain attacks, business email compromise, and large-scale data breaches. The rapid adoption of cloud services, remote work technologies, AI-driven applications, and interconnected digital ecosystems has significantly expanded organizational attack surfaces (World Economic Forum, 2025). Unlike conventional operational risks, cyber risks are dynamic and highly interconnected,

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768844
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

with a single incident capable of disrupting multiple business functions simultaneously. Consequently, cybersecurity is increasingly recognized as a strategic business risk requiring enterprise-wide governance rather than isolated technical management (ENISA, 2024; IBM Security, 2024).

Enterprise Risk Management (ERM) has emerged as a comprehensive governance approach that enables organizations to identify, assess, manage, monitor, and communicate risks that may affect strategic objectives. Frameworks such as COSO Enterprise Risk Management and ISO 31000 emphasize integrated risk governance, strategic alignment, organizational culture, and continuous risk monitoring. Unlike traditional risk management approaches that address risks independently, ERM provides a holistic view of organizational risk exposure, enabling executives to evaluate relationships among operational, financial, regulatory, technological, and strategic risks (COSO, 2017; ISO 31000, 2018). As digital transformation accelerates, cyber risk has become one of the most critical enterprise risks confronting modern organizations.

Despite this recognition, cybersecurity and enterprise risk management frequently remain organizationally separated. Cybersecurity functions often focus on technical activities such as vulnerability management, threat detection, security monitoring, and incident response, whereas ERM emphasizes governance, strategic objectives, organizational performance, and risk appetite. These differences have resulted in fragmented governance structures, separate reporting mechanisms, and inconsistent communication between cybersecurity professionals and executive leadership (NIST, 2024). Recent studies argue that integrating cybersecurity with ERM enhances organizational decision-making, improves resource allocation, and strengthens enterprise resilience by ensuring cyber risks are evaluated alongside other strategic risks (Stoneburner et al., 2023).

Cyber resilience has consequently emerged as a central concept linking cybersecurity and enterprise risk management. Unlike traditional cybersecurity, which primarily seeks to prevent attacks, cyber resilience focuses on an organization's ability to anticipate, withstand, respond to, recover from, and adapt to cyber disruptions while maintaining essential business operations. This broader perspective recognizes that complete prevention is unrealistic in today's threat environment. Instead, organizations must develop adaptive capabilities that support business continuity, rapid recovery, organizational learning, and continuous improvement following cyber incidents (World Economic Forum, 2025). Cyber resilience therefore extends cybersecurity beyond technology to encompass governance, leadership, organizational culture, and strategic planning.

Organizational resilience similarly emphasizes an organization's capacity to absorb disruptions, maintain critical operations, and adapt to changing conditions. Contemporary resilience literature views resilience as a multidimensional capability involving governance, operational flexibility, technological preparedness, and organizational learning. Within cybersecurity contexts, resilience depends on integrating technical security controls with enterprise governance, business continuity management, disaster recovery planning, and organizational risk management. Such integration enables organizations to minimize operational

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768844
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

disruption while sustaining long-term organizational performance despite evolving cyber threats.

Several internationally recognized cybersecurity frameworks provide structured guidance for improving cybersecurity governance. The NIST Cybersecurity Framework (CSF 2.0), ISO/IEC 27001:2022, CIS Critical Security Controls, and COBIT have become widely adopted standards for identifying vulnerabilities, implementing security controls, monitoring performance, and responding to incidents (NIST, 2024; ISO/IEC 27001, 2022; ISACA, 2023). Although these frameworks significantly strengthen organizational cybersecurity maturity, many primarily emphasize technical implementation and security controls. Consequently, organizations may achieve cybersecurity compliance while still lacking effective integration between cybersecurity activities and enterprise-wide governance or strategic decision-making.

Similarly, established ERM frameworks, including COSO ERM and ISO 31000, provide comprehensive guidance for enterprise governance, risk assessment, stakeholder engagement, and strategic risk management. However, these frameworks offer relatively limited guidance regarding cybersecurity-specific issues such as threat intelligence, digital infrastructure protection, cyber incident response, and vulnerability management. This limitation has encouraged researchers to advocate for integrated governance models that combine cybersecurity management with enterprise risk management to improve organizational resilience and governance effectiveness.

A recurring issue identified in recent literature is the persistence of organizational silos separating cybersecurity from enterprise risk management. Cybersecurity units frequently report through information technology structures, while enterprise risk management operates independently under executive or governance functions. Differences in governance structures, performance metrics, terminology, and reporting mechanisms often hinder communication and reduce enterprise-wide visibility of cyber risks. Researchers consistently argue that stronger executive leadership, cross-functional collaboration, integrated governance structures, and unified risk reporting are essential for overcoming these barriers and strengthening organizational resilience (PwC, 2024; McKinsey & Company, 2023).

Recent empirical studies further reinforce the strategic benefits of integrating cybersecurity and ERM. Organizations with mature cybersecurity governance and enterprise-wide risk management capabilities consistently demonstrate stronger cyber resilience, improved regulatory compliance, enhanced risk awareness, better investment prioritization, and faster recovery following cyber incidents (World Economic Forum, 2025; ENISA, 2024). Integrated governance enables cybersecurity investments to be aligned with organizational objectives, improving both operational efficiency and long-term organizational sustainability.

The theoretical foundation for this integration is supported by Resilience Theory, Socio-Technical Systems Theory, and Institutional Theory. Resilience Theory emphasizes adaptive capacity, recovery, and continuous learning; Socio-Technical Systems Theory highlights the interaction among technology, people, governance,

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768844
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

and organizational processes; while Institutional Theory explains how regulatory requirements, industry standards, and stakeholder expectations influence cybersecurity governance. Collectively, these theories suggest that effective cyber resilience depends on aligning technical controls with organizational governance and enterprise risk management rather than treating cybersecurity as an isolated technical function.

Although substantial progress has been made in cybersecurity governance and enterprise risk management research, an important gap remains regarding integrated frameworks that systematically combine cybersecurity, enterprise risk management, and organizational resilience within a unified governance model. Existing studies frequently examine these concepts independently, with limited attention to their practical integration across diverse organizational contexts. This study addresses this gap by proposing an Integrated Cybersecurity–Enterprise Risk Management Framework that aligns cybersecurity governance, enterprise risk management, and resilience capabilities to support sustainable organizational performance in increasingly complex digital environments.

3. Conceptual Foundations of Cybersecurity, Enterprise Risk Management, and Organizational Resilience

The rapid advancement of digital technologies has transformed cybersecurity from a technical function into a strategic organizational capability. Modern organizations increasingly depend on cloud computing, artificial intelligence (AI), the Internet of Things (IoT), data analytics, and interconnected digital infrastructures to support business operations and strategic objectives. Consequently, cyber threats now have far-reaching implications for operational continuity, regulatory compliance, stakeholder trust, and organizational competitiveness. Cybersecurity is therefore recognized as an integral component of corporate governance that must align with broader business objectives and enterprise-wide risk management.

The contemporary cyber threat environment is characterized by increasingly sophisticated attacks, including ransomware, phishing, insider threats, supply-chain compromises, and data breaches. These threats extend beyond information technology systems and can disrupt business operations, damage organizational reputation, incur regulatory sanctions, and reduce customer confidence. Because cyber risks are dynamic and interconnected, organizations increasingly acknowledge that traditional, technology-focused cybersecurity approaches are insufficient. Instead, cyber risk must be managed within a broader governance framework that supports strategic decision-making and organizational resilience.

Enterprise Risk Management (ERM) provides such a framework by promoting an integrated approach to identifying, assessing, managing, and monitoring organizational risks. Unlike traditional risk management, which often operates within functional silos, ERM encourages a holistic understanding of enterprise-wide risk exposure. Contemporary ERM frameworks emphasize governance, accountability, strategic alignment, risk culture, and continuous monitoring to improve organizational performance under uncertainty. Integrating cybersecurity into ERM enables organizations to evaluate cyber threats alongside financial, operational,

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768844
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

regulatory, and strategic risks, thereby strengthening executive oversight, improving resource allocation, and enhancing enterprise-wide risk visibility.

The integration of cybersecurity and ERM forms the basis for organizational resilience. Organizational resilience refers to an organization's capacity to anticipate, withstand, adapt to, and recover from disruptive events while maintaining critical business functions. Unlike conventional security approaches that primarily emphasize prevention, resilience recognizes that cyber incidents are inevitable and therefore requires organizations to develop adaptive capabilities that support rapid response, recovery, learning, and continuous improvement. Effective resilience depends on combining cybersecurity controls with governance, business continuity planning, disaster recovery, and enterprise risk management to sustain long-term organizational performance.

This study is underpinned by three complementary theoretical perspectives. **Resilience Theory** explains how organizations maintain performance under conditions of uncertainty by developing adaptive capabilities that support anticipation, absorption, recovery, and continuous learning following disruptive events. Within cybersecurity, the theory highlights the importance of integrating preventive, detective, responsive, and recovery-oriented capabilities into a coordinated governance structure that enhances operational continuity.

Socio-Technical Systems Theory argues that organizational performance results from the interaction of technological systems and social elements, including people, organizational culture, governance, and business processes. Effective cybersecurity therefore extends beyond technical controls and depends on employee awareness, leadership commitment, communication, and organizational practices. Integrating cybersecurity with ERM supports this perspective by aligning technology, governance, and organizational processes within a unified risk management framework.

Institutional Theory further explains how external pressures influence organizational cybersecurity practices. Regulatory requirements, industry standards, stakeholder expectations, and competitive pressures increasingly compel organizations to strengthen cybersecurity governance and demonstrate effective enterprise risk management. Consequently, many organizations integrate cybersecurity with ERM not only to improve operational resilience but also to achieve regulatory compliance, organizational legitimacy, and stakeholder confidence.

Collectively, cybersecurity, enterprise risk management, and organizational resilience constitute a mutually reinforcing governance system. Cybersecurity provides mechanisms for protecting information assets, detecting threats, and reducing vulnerabilities. ERM supplies the governance structures and decision-making processes required to evaluate cyber risks within the context of organizational objectives. Organizational resilience represents the outcome of these integrated capabilities by enabling organizations to sustain operations, adapt to changing threat environments, and recover effectively from cyber disruptions. Aligning cybersecurity with enterprise risk management therefore enhances

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768844
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

governance effectiveness, improves strategic decision-making, strengthens organizational resilience, and supports sustainable organizational performance in increasingly complex digital environments.

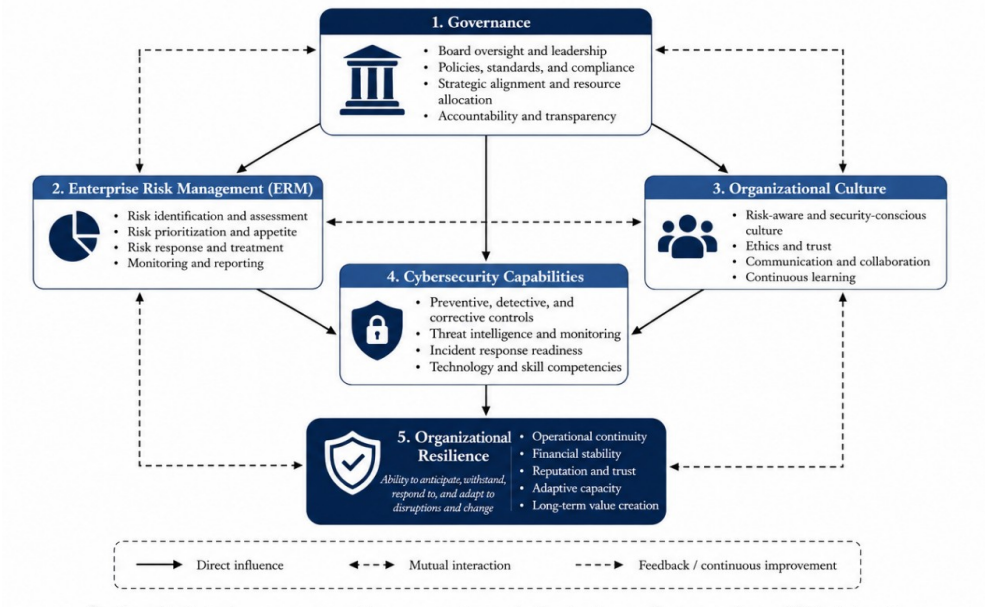


Figure 2: Theoretical Linkages among Cybersecurity, ERM, and Organizational Resilience

Source: Adopted from COSO

4. Methodology

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768844
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

This study adopts a qualitative conceptual research approach to develop an integrated framework that aligns cybersecurity and Enterprise Risk Management (ERM) for the purpose of enhancing organizational resilience. The choice of a qualitative methodology is informed by the exploratory and theory-building nature of the research. Unlike empirical studies that seek to test hypotheses using primary quantitative data, conceptual studies focus on synthesizing existing knowledge, identifying relationships among concepts, and proposing frameworks that can guide future research and organizational practice. Given that the objective of this study is to develop a comprehensive framework integrating cybersecurity and enterprise risk management within a resilience-oriented governance structure, a qualitative conceptual design provides an appropriate methodological foundation.

The study is grounded in an interpretivist research philosophy, which emphasizes understanding complex organizational phenomena through the interpretation of existing knowledge, theories, and documented evidence. Interpretivism is particularly suitable for studies involving governance, risk management, and organizational resilience because these concepts are influenced by contextual, organizational, and environmental factors that cannot be adequately understood through purely quantitative measures. By adopting this philosophical perspective, the study seeks to explore how cybersecurity, enterprise risk management, and organizational resilience interact conceptually and how these interactions can be integrated into a unified framework capable of addressing contemporary organizational challenges.

A doctrinal and literature-based research design was employed to facilitate a systematic examination of relevant theoretical, conceptual, and practical knowledge. Doctrinal research is widely used in policy, governance, and management studies to analyze existing frameworks, standards, models, and institutional practices. In this study, the doctrinal approach enabled the examination of established cybersecurity frameworks, enterprise risk management models, resilience theories, and governance principles that collectively inform the development of the proposed framework. The design also supports the identification of strengths, limitations, and gaps within existing approaches to cybersecurity and risk management integration.

Data for the study were obtained exclusively from secondary sources. These sources included peer-reviewed journal articles, conference proceedings, academic books, industry reports, professional publications, international standards, and organizational guidance documents published between 2020 and 2026. Particular emphasis was placed on literature relating to cybersecurity governance, enterprise risk management, organizational resilience, cyber resilience, risk governance, business continuity management, and integrated risk management frameworks. In addition, internationally recognized standards and frameworks, including the NIST Cybersecurity Framework, ISO 27001, ISO 31000, COSO Enterprise Risk Management Framework, COBIT, and related governance models, were reviewed to provide practical and theoretical insights relevant to framework development.

The literature selection process followed a structured review procedure. Relevant publications were identified through academic databases, digital libraries, institutional repositories, and professional publications. Inclusion criteria focused on sources that directly addressed cybersecurity management, enterprise risk

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768844
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

management, organizational resilience, governance frameworks, and risk integration. Priority was given to recent publications to ensure that the study reflected contemporary developments in cybersecurity and organizational risk management. Sources that lacked relevance to the study objectives or did not contribute significantly to the conceptual understanding of the research problem were excluded from the review process.

Data analysis was conducted using thematic analysis. This analytical approach involved the systematic identification, categorization, and interpretation of recurring concepts and themes within the reviewed literature. The analysis focused on identifying key dimensions of cybersecurity governance, enterprise risk management practices, organizational resilience capabilities, and existing integration approaches. Through this process, common patterns, relationships, and conceptual linkages were identified and synthesized into broader thematic categories. These themes subsequently served as the building blocks for the development of the proposed integrated cybersecurity–ERM framework.

The framework development process involved a multi-stage conceptual synthesis. First, relevant theoretical foundations, including Resilience Theory, Socio-Technical Systems Theory, Institutional Theory, and Enterprise Risk Management principles, were examined to establish a theoretical basis for integration. Second, recurring themes identified through the literature review were analyzed to determine critical components required for effective cybersecurity and risk management integration. Third, these components were organized into a structured framework illustrating the relationships among governance, cyber risk assessment, cybersecurity controls, incident response, business continuity, continuous monitoring, and organizational resilience outcomes. Finally, the proposed framework was evaluated conceptually against existing literature to ensure coherence, relevance, and practical applicability.

To enhance the credibility and rigor of the study, multiple sources of evidence were utilized to facilitate triangulation and reduce potential bias. The integration of scholarly literature, professional standards, and industry guidance contributed to a balanced and comprehensive understanding of the subject matter. Furthermore, the study adhered to accepted principles of academic integrity through objective analysis, accurate attribution of sources, and transparent interpretation of findings. Since the research relied exclusively on publicly available secondary data and did not involve human participants, no ethical risks requiring formal ethical approval were identified. This methodological approach provides a robust foundation for developing an integrated cybersecurity–ERM framework capable of supporting organizational resilience in increasingly complex and digitally dependent environments.

5. Development of the Integrated Cybersecurity–ERM Framework and Discussion

The increasing complexity of cyber threats and the growing interdependence between digital technologies and organizational operations necessitate a more integrated approach to risk management. The literature reviewed in this study indicates that although cybersecurity and Enterprise Risk Management (ERM) share similar objectives relating to risk identification, assessment, mitigation, and monitoring, they

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768844
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

are frequently implemented as separate organizational functions. This separation often results in fragmented governance structures, inconsistent risk communication, duplication of effort, and limited organizational visibility into cyber-related risks. Consequently, organizations may struggle to align cybersecurity investments with strategic objectives or adequately prepare for cyber incidents that have enterprise-wide implications. To address these challenges, this study proposes an Integrated Cybersecurity–ERM Framework designed to align cybersecurity governance, enterprise risk management processes, and organizational resilience objectives within a unified structure.

The proposed framework is founded on the principle that cybersecurity should be treated as an enterprise-wide strategic risk rather than solely as a technical issue. By embedding cybersecurity within broader risk governance structures, organizations can improve decision-making, strengthen accountability, and enhance resilience against evolving cyber threats. The framework draws upon the theoretical foundations discussed earlier, including Resilience Theory, Socio-Technical Systems Theory, and Institutional Theory, as well as established cybersecurity and risk management standards such as the NIST Cybersecurity Framework, ISO 27001, ISO 31000, and COSO ERM. These foundations provide the conceptual basis for integrating technological, organizational, governance, and resilience-oriented dimensions into a comprehensive risk management model.

The first component of the framework is governance and strategic oversight. Effective governance serves as the foundation upon which all cybersecurity and risk management activities are built. Governance ensures that cybersecurity objectives are aligned with organizational strategy, risk appetite, regulatory obligations, and stakeholder expectations. Within the proposed framework, boards of directors and senior management assume primary responsibility for establishing cybersecurity priorities, allocating resources, defining risk tolerance levels, and overseeing risk management performance. This governance-oriented approach addresses one of the most common weaknesses identified in the literature, namely the tendency to delegate cybersecurity responsibilities exclusively to technical departments without sufficient executive oversight. Integrating governance structures enables cybersecurity risks to be evaluated alongside other strategic risks, thereby improving organizational accountability and decision-making.

The second component focuses on integrated risk identification and assessment. Organizations operate in environments characterized by multiple interconnected risks, including operational, financial, strategic, legal, reputational, and technological threats. The proposed framework emphasizes the need for cyber risks to be identified, assessed, and prioritized within broader enterprise risk assessment processes. Rather than conducting cybersecurity assessments independently, organizations should integrate cyber risk evaluations into enterprise-wide risk registers and risk reporting mechanisms. This integration facilitates a more comprehensive understanding of risk interdependencies and enables decision-makers to allocate resources according to overall organizational risk exposure. Furthermore, continuous risk assessment supports proactive identification of emerging vulnerabilities associated with evolving technologies, supply-chain dependencies, and changing threat landscapes.

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768844
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

A third component of the framework involves cybersecurity controls and risk treatment mechanisms. Once cyber risks have been identified and assessed, organizations must implement appropriate preventive, detective, and corrective controls. The framework emphasizes a risk-based approach to control selection, ensuring that cybersecurity investments are aligned with organizational priorities and risk exposure levels. Security controls may include access management systems, network security technologies, encryption mechanisms, vulnerability management programs, security awareness training, threat intelligence capabilities, and security monitoring tools. Integrating these controls within ERM processes enables organizations to evaluate cybersecurity investments based on their contribution to enterprise objectives and resilience outcomes rather than solely on technical considerations. This alignment enhances the effectiveness of cybersecurity spending and promotes greater strategic coherence.

The fourth component is incident response and crisis management. Despite significant investments in preventive controls, organizations cannot eliminate cyber risks entirely. Consequently, effective incident response capabilities are essential for minimizing the impact of cyber incidents and supporting operational continuity. The proposed framework incorporates incident response as a core element of enterprise risk management, ensuring that cyber incidents are addressed through coordinated organizational procedures rather than isolated technical actions. Incident response planning includes threat detection, escalation procedures, communication protocols, stakeholder engagement, forensic investigation, and post-incident evaluation. Integrating these activities within broader crisis management structures enables organizations to respond more effectively to cyber disruptions and reduce recovery times.

Business continuity and recovery planning constitute the fifth component of the framework. Organizational resilience depends not only on preventing incidents but also on maintaining essential operations during periods of disruption. Business continuity planning ensures that critical functions can continue despite cyber incidents, while recovery planning focuses on restoring systems, services, and operational capabilities following disruptions. The proposed framework integrates business continuity and disaster recovery considerations directly into cybersecurity and enterprise risk management processes. This integration ensures that resilience objectives are embedded throughout organizational planning and decision-making activities. By linking continuity planning with cyber risk assessments, organizations can prioritize recovery resources and establish realistic recovery objectives aligned with business requirements.

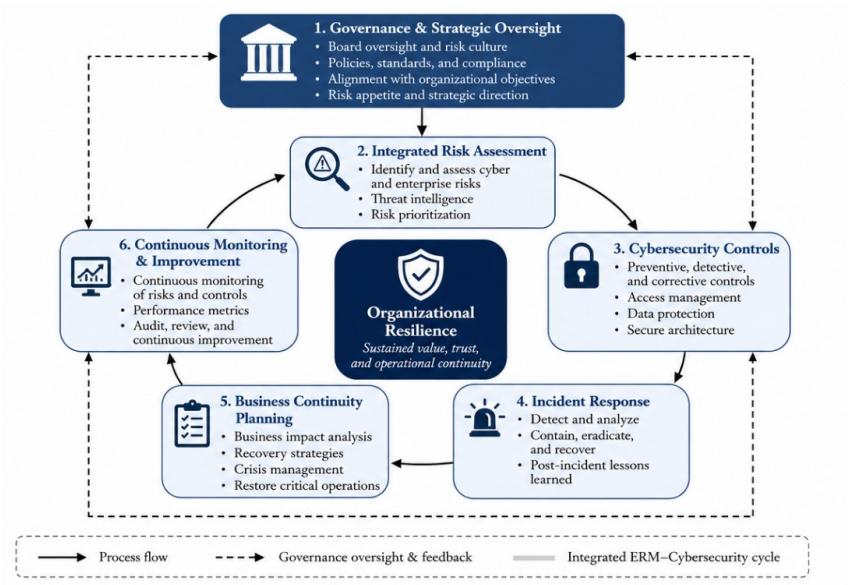
The sixth component involves continuous monitoring, performance evaluation, and organizational learning. Cyber threats evolve rapidly, requiring organizations to maintain ongoing visibility into their security posture and risk environment. Continuous monitoring enables organizations to identify emerging vulnerabilities, evaluate control effectiveness, and detect unusual activities that may indicate security incidents. The framework emphasizes the importance of establishing performance indicators, conducting regular audits, performing security assessments, and reviewing risk management outcomes. Organizational learning is equally important because resilience is strengthened when institutions systematically analyze incidents, identify

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768844
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

lessons learned, and adapt their policies and procedures accordingly. Continuous improvement therefore serves as a critical mechanism for maintaining long-term effectiveness and relevance within dynamic threat environments.

Table 3: Components of the Proposed Integrated Cybersecurity–ERM Framework

Framework Component	Primary Purpose	Expected Organizational Outcome
Governance and Strategic Oversight	Align cybersecurity with organizational strategy and risk appetite	Improved accountability and executive decision-making
Integrated Risk Identification and Assessment	Identify and evaluate cyber risks within enterprise risk structures	Enhanced risk visibility and prioritization
Cybersecurity Controls and Risk Treatment	Implement controls to mitigate identified cyber risks	Reduced vulnerability exposure and improved security posture
Incident Response and Crisis Management	Coordinate response activities during cyber incidents	Faster containment and reduced operational disruption
Business Continuity and Recovery Planning	Maintain critical operations and restore services	Improved resilience and recovery capability
Continuous Monitoring and Organizational Learning	Evaluate performance and support continuous improvement	Adaptive resilience and long-term risk management effectiveness



ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768844
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

Figure 3. Proposed Integrated Cybersecurity–ERM Framework

Source: Adopted from COSO (2017) Enterprise Risk Management: Integrating with Strategy and Performance; NIST (2023) Cybrsecurity Framork 2.0; ISO (2022) ISO 31000:2018 Risk Management Guidelines; ISO (2019) ISO/IEC 27001:2013

The proposed framework contributes to existing knowledge by addressing limitations identified in both cybersecurity and enterprise risk management literature. Existing cybersecurity frameworks often concentrate on technical security controls without sufficiently addressing enterprise-wide governance and strategic alignment. Conversely, many ERM frameworks recognize cyber risk as an important organizational concern but provide limited guidance regarding cybersecurity-specific implementation requirements. The integrated framework bridges this gap by establishing clear relationships among governance structures, risk management processes, cybersecurity capabilities, and resilience outcomes. This holistic perspective enables organizations to manage cyber risks more effectively while supporting broader organizational objectives.

From a practical perspective, the framework offers organizations a structured approach for embedding cybersecurity into enterprise governance and decision-making processes. One of its primary advantages is the promotion of cross-functional collaboration among executive leadership, risk managers, cybersecurity professionals, operational managers, and business continuity teams. Such collaboration reduces organizational silos and facilitates more effective communication regarding cyber risks and resilience priorities. Furthermore, the framework supports improved resource allocation by ensuring that cybersecurity investments are guided by enterprise-wide risk assessments rather than isolated departmental concerns.

The framework also addresses the growing need for organizational resilience in increasingly uncertain environments. As cyber threats continue to evolve and digital transformation accelerates, organizations require adaptive capabilities that enable them to anticipate, withstand, recover from, and learn from disruptions. The integrated framework supports these objectives by combining preventive security measures with responsive and recovery-oriented capabilities. This balanced approach

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768844
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

reflects contemporary resilience thinking, which recognizes that resilience depends not only on protection but also on adaptability, recovery, and continuous improvement.

Table 4: **Expected Organizational Benefits of Framework Adoption**

Benefit	Cybersecurity Impact	Organizational Impact
Improved Governance	Stronger cybersecurity oversight	Better strategic decision-making
Enhanced Risk Visibility	Comprehensive cyber risk assessment	Improved enterprise risk awareness
Better Resource Allocation	Risk-based security investments	Increased operational efficiency
Stronger Incident Response	Faster detection and containment	Reduced disruption and losses
Improved Business Continuity	Enhanced recovery capabilities	Greater organizational resilience
Continuous Improvement	Adaptive security posture	Long-term sustainability and competitiveness

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768844
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

Figure 4. Framework Implementation Cycle

Source: Adopted from NIST Cybersecurity Framework (Version 2.0) (NIST, 2024); ISO/IEC 27001:2022 (ISO, 2022); and ENISA Cybersecurity Culture Guidelines (ENISA, 2022).

The proposed Integrated Cybersecurity–ERM Framework demonstrates that organizational resilience can be significantly enhanced when cybersecurity and enterprise risk management are treated as complementary and mutually reinforcing disciplines. By aligning governance, risk assessment, security controls, response capabilities, continuity planning, and continuous improvement within a unified structure, organizations can strengthen their ability to manage cyber risks, sustain operations, and adapt to emerging challenges in increasingly complex digital environments.

6. Conclusion

This study developed an **Integrated Cybersecurity–Enterprise Risk Management (ERM) Framework** to strengthen cybersecurity governance, enterprise risk management, and organizational resilience. The findings indicate that cybersecurity and ERM are closely interconnected, yet many organizations continue to manage them independently, resulting in fragmented governance and reduced cyber resilience. The proposed framework integrates governance, risk assessment, cybersecurity controls, incident response, business continuity, and continuous monitoring into a unified approach that enhances risk visibility, strategic decision-making, and organizational resilience. Grounded in **Resilience Theory**, **Socio-Technical Systems Theory**, and **Institutional Theory**, the framework provides both a theoretical and practical foundation for aligning cybersecurity with enterprise objectives. Future research should empirically validate the framework across different industries and investigate the role of emerging technologies, including artificial intelligence and cloud computing, in enhancing integrated cyber risk management.

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768844
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

7. Recommendations

Organizations should integrate cybersecurity into enterprise risk management by strengthening governance, embedding cyber risks within strategic planning and risk registers, and promoting collaboration among cybersecurity, risk management, and executive teams. Continuous investment in cybersecurity controls, employee awareness, business continuity, and incident response capabilities should be supported by regular resilience assessments and performance monitoring. Regulators should encourage integrated cybersecurity and ERM practices through harmonized governance standards and resilience-focused guidance to strengthen organizational sustainability in an increasingly digital environment.

Acknowledgements

References

Aven, T. (2021). *Risk assessment and risk management: Review of recent advances on their foundation*. European Journal of Operational Research, 253(1), 1–13.

Bada, M., Nurse, J. R. C., & Goldsmith, M. (2021). Cybersecurity awareness campaigns: Why do they fail to change behaviour? *International Journal of Information Management, 58*, 102280.

Bouveret, A. (2020). *Cyber risk for the financial sector: A framework for quantitative assessment*. International Monetary Fund.

Boyes, H. (2021). The cyber security body of knowledge and organisational resilience. *Computers & Security, 105*, 102241.

Central Bank of Nigeria. (2023). *Risk-based cybersecurity framework and guidelines for financial institutions*. Central Bank of Nigeria.

Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise risk management: Integrating with strategy and performance*. COSO.

Crawford, M., & Jabbour, C. (2022). Enterprise risk management and organizational resilience in the digital era. *Journal of Risk Research, 25*(8), 1054–1072.

Cybersecurity and Infrastructure Security Agency. (2023). *Cybersecurity performance goals*. CISA.

ENISA. (2023). *ENISA threat landscape 2023*. European Union Agency for Cybersecurity.

ENISA. (2024). *Cybersecurity and resilience trends report 2024*. European Union Agency for Cybersecurity.

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768844
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

Ghadge, A., Wei, H., Caldwell, N., & Wilding, R. (2022). Managing cyber risk in supply chains through integrated risk governance. *Supply Chain Management: An International Journal, 27*(4), 531–547.

Greitzer, F. L., & Frincke, D. A. (2021). Combating the insider cyber threat. *IEEE Security & Privacy, 19*(1), 61–64.

Herath, T., & Herath, H. (2020). Coping with cyber threats: Integration of enterprise risk management and information security. *Information Systems Management, 37*(2), 120–134.

IBM Security. (2024). *Cost of a data breach report 2024*. IBM Corporation.

Institute of Risk Management. (2022). *Risk appetite and resilience guidance*. IRM.

International Organization for Standardization. (2018). *ISO 31000: Risk management —Guidelines*. ISO.

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

International Organization for Standardization. (2022). *ISO 22301: Security and resilience—Business continuity management systems—Requirements*. ISO.

ISACA. (2023). *State of cybersecurity 2023*. ISACA.

Kaplan, R. S., & Mikes, A. (2021). Risk management: The reinvention of risk management in the digital age. *Harvard Business Review, 99*(3), 48–57.

Kshetri, N. (2021). Cybersecurity management in developing and developed economies. *Journal of Global Information Technology Management, 24*(2), 81–89.

Lundqvist, S. A. (2020). Why firms implement risk governance frameworks. *Risk Management, 22*(2), 121–139.

McKinsey & Company. (2023). *Cybersecurity trends outlook 2023*. McKinsey & Company.

Mikes, A., & Kaplan, R. S. (2020). Toward a contingency theory of enterprise risk management. *Management Accounting Research, 46*, 100643.

National Institute of Standards and Technology. (2024). *Integrating cybersecurity and enterprise risk management (NISTIR 8286 Rev. 1)*. U.S. Department of Commerce.

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768844
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

Nielsen, M., & Madsen, S. (2022). Enterprise risk management and digital resilience: Emerging perspectives. *International Journal of Risk Assessment and Management, 25*(1), 45–62.

NIST. (2023). *Cybersecurity and privacy reference tool*. National Institute of Standards and Technology.

OECD. (2023). *Digital security risk management for economic and social prosperity*. Organisation for Economic Co-operation and Development.

Olaniyi, O., & Reidolf, M. (2021). Cybersecurity governance and organizational performance: A strategic perspective. *Journal of Information Security and Applications, 58*, 102754.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2020). Determining employee awareness using cybersecurity culture assessments. *Computers & Security, 94*, 101817.

PwC. (2024). *Global digital trust insights 2024*. PricewaterhouseCoopers.

Radanliev, P., De Roure, D., Walton, R., Van Kleek, M., Santos, O., & Ani, U. (2020). Artificial intelligence and cyber risk management. *AI & Society, 35*(4), 1045–1058.

Reason, J. (2020). Human error and organizational resilience in complex systems. *Safety Science, 130*, 104874.

Scott, W. R. (2022). *Institutions and organizations: Ideas, interests, and identities* (5th ed.). Sage Publications.

Sheffi, Y. (2021). *The new (ab)normal: Reshaping business and supply chain strategy beyond COVID-19*. MIT Press.

Stoneburner, G., Goguen, A., & Feringa, A. (2023). Risk management guide for information technology systems. *Information Security Journal, 32*(2), 65–79.

Taleb, N. N. (2021). *Antifragile: Things that gain from disorder* (2nd ed.). Random House.

Trompeter, C., Vieru, D., & Chanal, V. (2022). Cyber resilience and organizational adaptation in uncertain environments. *Technological Forecasting and Social Change, 181*, 121764.

Von Solms, R., & Van Niekerk, J. (2021). From information security to cybersecurity. *Computers & Security, 38*, 97–102.

World Economic Forum. (2025). *Global cyber security outlook 2025*. World Economic Forum.

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768844
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

World Bank. (2022). *Cybersecurity and digital development in emerging economies*. World Bank.

Yaraghi, N., & Sharman, R. (2021). Enterprise cybersecurity and organizational resilience. *Journal of Cyber Policy, 6*(3), 337–353.

Zhang, Y., Xue, Y., & Dhaliwal, J. (2022). Aligning cybersecurity governance with enterprise risk management. *Information & Management, 59*(5), 103654.

Zwikael, O., & Meredith, J. R. (2021). Organizational resilience and risk management capabilities. *International Journal of Project Management, 39*(4), 349–360.