ISSN: 2971-7760 | VOL 6, ISS 3 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21770424
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

Comparative Analysis of Cybersecurity Frameworks (NIST, ISO/IEC 27001) in Supporting Enterprise Risk Management Objectives

Sulaiman Sani

Department of Computer Science
Federal Polytechnic Mubi, P.M.B. 35, Mubi
Adamawa State

08136835923

Email: suleimanp2@gmail.com

tetfund
TERTIARY EDUCATION TRUST FUND

Abstract

The increasing frequency and sophistication of cyber threats have elevated cybersecurity from a purely technical function to a strategic organizational priority. Consequently, organizations increasingly integrate cybersecurity governance into Enterprise Risk Management (ERM) frameworks to enhance resilience, ensure regulatory compliance, and achieve organizational objectives. Among the most widely adopted cybersecurity frameworks are the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF 2.0) and the International Organization for Standardization's ISO/IEC 27001:2022 Information Security Management System (ISMS). This study comparatively analyses the extent to which these frameworks support Enterprise Risk Management objectives. Adopting a qualitative comparative research design based on doctrinal and systematic literature analysis, the study examines the governance structures, risk management approaches, implementation mechanisms, regulatory alignment, and organizational applicability of both frameworks. The analysis demonstrates that while NIST CSF 2.0 provides a flexible, risk-based framework emphasizing governance, cyber resilience, and continuous improvement, ISO/IEC 27001:2022 offers a structured and certifiable management system that strengthens information security governance through standardized controls and continual performance evaluation. The study further reveals that neither framework independently addresses all dimensions of enterprise risk management; however, their complementary implementation significantly enhances strategic decision-making, operational resilience, regulatory compliance, and organizational sustainability. The paper concludes that organizations seeking comprehensive cyber risk governance should adopt an integrated implementation strategy that leverages the flexibility of NIST CSF 2.0 alongside the structured management processes of ISO/IEC 27001:2022 to achieve broader Enterprise Risk Management objectives.

ISSN: 2971-7760 | VOL 6, ISS 3 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21770424
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

Keywords: Cybersecurity Governance, Enterprise Risk Management, NIST Cybersecurity Framework 2.0, ISO/IEC 27001:2022, Information Security Management System, Organizational Resilience, Cyber Risk.

1. Introduction

Digital transformation has fundamentally reshaped the manner in which modern organizations conduct business, deliver services, manage information assets, and interact with stakeholders. The increasing adoption of cloud computing, artificial intelligence, the Internet of Things (IoT), big data analytics, mobile technologies, and interconnected digital ecosystems has generated unprecedented opportunities for innovation and organizational growth. However, these technological advancements have simultaneously expanded organizations' exposure to cyber threats, including ransomware attacks, phishing campaigns, insider threats, supply chain compromises, data breaches, and attacks on critical infrastructure (National Institute of Standards and Technology [NIST], 2024; International Organization for Standardization [ISO], 2022).

Cybersecurity has therefore evolved beyond its traditional technical orientation to become a fundamental component of enterprise governance and strategic risk management. Contemporary organizations increasingly recognize cyber risk as an enterprise-wide risk capable of affecting financial performance, regulatory compliance, operational continuity, corporate reputation, stakeholder confidence, and long-term organizational sustainability (Committee of Sponsoring Organizations of the Treadway Commission [COSO], 2017; World Economic Forum, 2025). Consequently, boards of directors and executive management are expected to integrate cybersecurity governance into Enterprise Risk Management (ERM) frameworks to ensure that cyber risks are identified, assessed, mitigated, monitored, and communicated within the broader context of organizational objectives.

Enterprise Risk Management provides organizations with a structured approach for identifying uncertainties that may influence the achievement of strategic, operational, reporting, and compliance objectives (COSO, 2017; ISO, 2018). Rather than treating cybersecurity as an isolated information technology function, ERM emphasizes integrating cyber risks with other organizational risks, including financial, operational, legal, reputational, environmental, and strategic risks. Such integration enables organizational leaders to allocate resources more effectively, improve decision-making processes, strengthen governance structures, and enhance organizational resilience against an increasingly dynamic threat landscape (Hopkin, 2024).

To support effective cybersecurity governance, organizations rely on internationally recognized cybersecurity frameworks that provide structured guidance for managing cyber risks. Among the most influential frameworks are the **NIST Cybersecurity Framework (CSF) 2.0**,

ISSN: 2971-7760 | VOL 6, ISS 3 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21770424
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

published by the National Institute of Standards and Technology in 2024, and **ISO/IEC 27001:2022**, the globally recognized standard for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). Although both frameworks pursue the common objective of strengthening cybersecurity governance, they differ in philosophy, implementation methodology, certification requirements, governance orientation, and organizational application (NIST, 2024; ISO, 2022).

The NIST Cybersecurity Framework 2.0 adopts a flexible, risk-based approach organized around six core functions—**Govern, Identify, Protect, Detect, Respond, and Recover**—which collectively support organizational cyber resilience and risk-informed decision-making (NIST, 2024). By contrast, ISO/IEC 27001:2022 provides a formal management system based on the Plan–Do–Check–Act (PDCA) cycle, emphasizing risk assessment, documented controls, continual improvement, internal auditing, management review, and independent certification. While the NIST framework offers considerable flexibility suitable for organizations of varying sizes and sectors, ISO/IEC 27001 provides internationally recognized assurance through certification and standardized information security governance (ISO, 2022).

Despite the widespread adoption of both frameworks, existing literature predominantly evaluates NIST CSF and ISO/IEC 27001 independently, often emphasizing technical implementation or information security controls without adequately examining their comparative contribution to Enterprise Risk Management objectives. Furthermore, relatively limited attention has been devoted to understanding how these frameworks complement one another in strengthening organizational governance, strategic decision-making, compliance management, operational resilience, and enterprise-wide risk integration across diverse organizational contexts, particularly in developing economies.

This study addresses this gap by undertaking a comparative analysis of the NIST Cybersecurity Framework 2.0 and ISO/IEC 27001:2022 in supporting Enterprise Risk Management objectives. Specifically, the study evaluates the governance principles, risk management capabilities, implementation characteristics, strengths, limitations, and practical implications of both frameworks while identifying opportunities for integrated implementation that enhance organizational resilience and enterprise-wide cyber risk governance. The findings contribute to the growing body of knowledge on cybersecurity governance by providing evidence-based guidance for organizational leaders, Chief Information Security Officers, risk managers, auditors, policymakers, and researchers seeking to align cybersecurity initiatives with broader Enterprise Risk Management objectives.

2. Literature Review

ISSN: 2971-7760 | VOL 6, ISS 3 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21770424
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

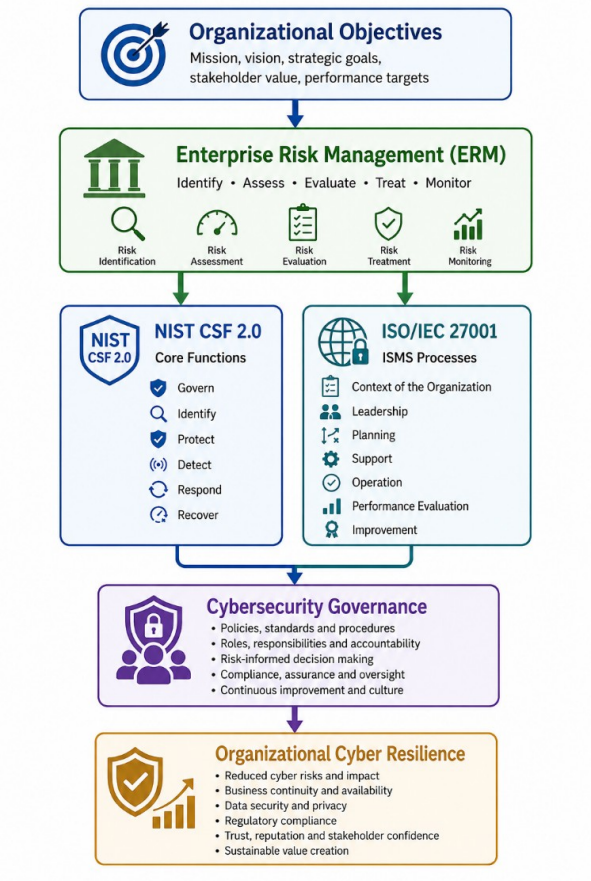
Cybersecurity governance has become a strategic organizational function that ensures cybersecurity activities align with business objectives, regulatory requirements, and enterprise risk management (ERM). Unlike traditional information security, which primarily focuses on technical safeguards, cybersecurity governance incorporates executive oversight, accountability, policy development, risk appetite, stakeholder engagement, and continuous performance evaluation (NIST, 2024; ISO, 2022). The growing frequency and sophistication of cyber threats have elevated cybersecurity from an operational IT concern to a board-level governance responsibility requiring continuous executive involvement (World Economic Forum, 2025).

Recent governance frameworks reinforce this strategic perspective. The NIST Cybersecurity Framework (CSF) 2.0 introduced the **Govern** function to strengthen executive accountability and integrate cybersecurity into enterprise-wide decision-making. Likewise, ISO/IEC 27001:2022 embeds governance within an Information Security Management System (ISMS) through leadership commitment, risk-based planning, continual improvement, and performance evaluation. While NIST CSF 2.0 provides a flexible, risk-based governance model, ISO/IEC 27001 offers an internationally recognized certifiable management system. Together, both frameworks promote governance maturity, organizational resilience, and continuous cyber risk management.

Enterprise Risk Management provides the organizational mechanism for identifying, assessing, prioritizing, and monitoring risks that may affect strategic objectives (COSO, 2017; ISO, 2018). Modern organizations increasingly recognize cybersecurity as an enterprise risk rather than solely an information technology issue. Consequently, integrating cybersecurity within ERM enables organizations to evaluate cyber risks alongside financial, operational, legal, strategic, and reputational risks, thereby improving governance, resource allocation, and executive decision-making.

The convergence of cybersecurity governance and ERM has therefore become essential for organizational resilience. Cybersecurity generates timely threat intelligence, while ERM translates that intelligence into enterprise-wide risk information capable of supporting strategic decisions. Recent NIST guidance promotes this integration by encouraging organizations to communicate cyber risks using a common enterprise governance language that improves coordination among executive management, boards of directors, cybersecurity professionals, and risk managers.

ISSN: 2971-7760 | VOL 6, ISS 3 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21770424
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA



ISSN: 2971-7760 | VOL 6, ISS 3 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21770424
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

Figure 1: Integration of Cybersecurity Governance and Enterprise Risk Management
Source: Developed by the Author (2026), adapted from NIST CSF 2.0 and ISO/IEC 27001:2022.

Empirical studies consistently demonstrate that governance maturity improves cybersecurity performance and organizational resilience. Alshaikh (2020) reported that effective cybersecurity governance enhances resilience, while Kure et al. (2021) emphasized that integrated governance strengthens organizational preparedness. ENISA (2021), ISO (2022), and ISACA (2022) similarly concluded that leadership commitment and governance maturity improve cybersecurity outcomes and digital trust. More recent studies indicate that NIST CSF 2.0 and ISO/IEC 27001 complement one another by combining flexible risk management with structured information security governance (McIntosh et al., 2024). Industry reports by Gartner (2025) and Deloitte (2025) further highlight that executive oversight and integrated governance significantly improve organizational cyber resilience.

ISSN: 2971-7760 | VOL 6, ISS 3 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21770424
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

Table 1. Selected Empirical Studies on Cybersecurity Governance and ERM

Authors	Focus	Key Finding
Alshaikh (2020)	Cybersecurity governance	Governance improves organizational resilience.
Kure et al. (2021)	Cyber resilience	Integrated governance strengthens resilience.
ENISA (2021)	Cybersecurity maturity	Governance determines organizational maturity.
ISO (2022)	ISMS implementation	ISO 27001 strengthens governance.
ISACA (2022)	Digital trust	Governance enhances stakeholder confidence.
McIntosh et al. (2024)	Governance frameworks	NIST and ISO provide complementary approaches.
Gartner (2025)	Cyber risk management	Executive oversight improves resilience.
Deloitte (2025)	Digital risk governance	Integrated governance strengthens organizational resilience.

Despite these advances, important gaps remain. Existing studies largely evaluate NIST CSF 2.0 and ISO/IEC 27001 independently, with limited attention to their complementary contribution to Enterprise Risk Management. Furthermore, empirical evidence examining integrated cybersecurity governance in developing economies remains relatively limited. This study addresses these gaps by comparatively evaluating NIST CSF 2.0 and ISO/IEC 27001:2022 from an Enterprise Risk Management perspective, highlighting their complementary strengths and implications for organizational governance and cyber resilience.

3. Comparative Framework Analysis

The NIST Cybersecurity Framework (CSF) 2.0 and ISO/IEC 27001:2022 are among the most widely adopted cybersecurity frameworks for improving organizational governance, risk management, and cyber resilience. Although both frameworks seek to strengthen cybersecurity, they differ in implementation philosophy, governance structure, and organizational application (NIST, 2024; ISO, 2022).

NIST CSF 2.0 adopts a flexible, outcomes-based approach built around six core functions—**Govern, Identify, Protect, Detect, Respond, and Recover**. The introduction of the **Govern** function strengthens executive accountability by integrating cybersecurity into enterprise strategy and Enterprise Risk Management (ERM). In contrast, ISO/IEC 27001:2022 establishes a certifiable Information Security Management System (ISMS) based on documented policies, risk assessment, internal auditing, and continual improvement. While NIST emphasizes governance flexibility, ISO/IEC 27001 provides a structured management system that enables

ISSN: 2971-7760 | VOL 6, ISS 3 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21770424
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

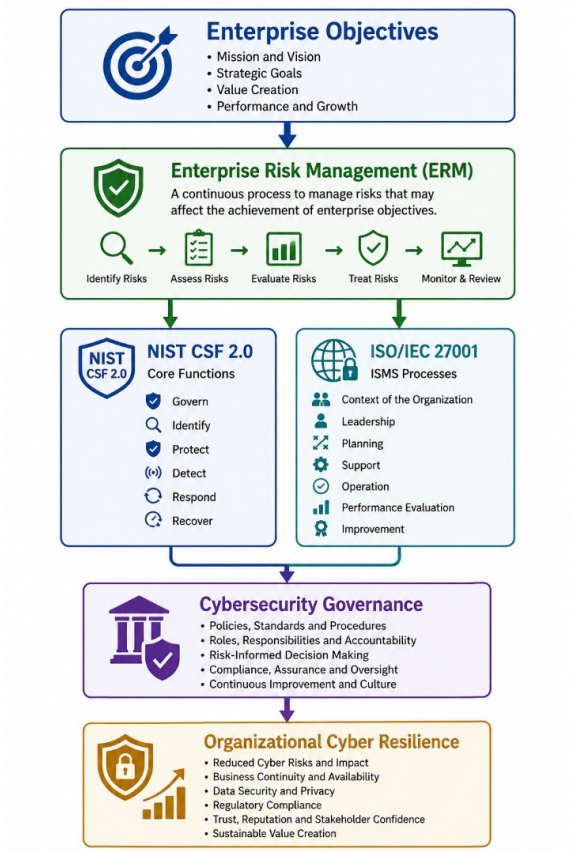
organizations to demonstrate compliance through international certification.

From an ERM perspective, the two frameworks are complementary rather than competing. NIST CSF 2.0 enhances enterprise governance by translating cybersecurity into strategic business risk, thereby improving executive decision-making and risk prioritization. ISO/IEC 27001 institutionalizes cybersecurity through standardized processes, documented controls, and continuous performance evaluation. Together, they strengthen governance, improve cyber risk visibility, support regulatory compliance, and enhance organizational resilience.

Table 2. Comparative Analysis of NIST CSF 2.0 and ISO/IEC 27001:2022

Evaluation Criterion	NIST CSF 2.0	ISO/IEC 27001:2022
Primary Focus	Cybersecurity risk management	Information Security Management System
Governance	Govern function	Leadership and management commitment
Risk Management	Adaptive and risk-based	Risk-based with formal documentation
Certification	Not certifiable	Internationally certifiable
Implementation	Highly flexible	Structured implementation
Continuous Improvement	Continuous governance	PDCA improvement cycle
Executive Involvement	Strong	Mandatory
Organizational Suitability	All sectors	Organizations requiring certification

ISSN: 2971-7760 | VOL 6, ISS 3 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21770424
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA



Source: Developed by the Author (2026), synthesized from NIST (2024) and ISO/IEC 27001:2022.

ISSN: 2971-7760 | VOL 6, ISS 3 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21770424
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

Figure 2: Alignment of Cybersecurity Frameworks with Enterprise Risk Management

Source: Developed by the Author (2026).

The comparative analysis indicates that neither framework independently satisfies all organizational cybersecurity requirements. NIST CSF 2.0 provides strategic flexibility and enterprise-wide governance, whereas ISO/IEC 27001 delivers operational discipline through a certifiable management system. An integrated implementation therefore offers the greatest value by combining NIST's governance-oriented approach with ISO/IEC 27001's structured controls and continual improvement mechanisms. Such integration strengthens Enterprise Risk Management, supports regulatory compliance, enhances executive decision-making, and improves long-term organizational cyber resilience.

4. Discussion and Practical Implications

The comparative analysis demonstrates that cybersecurity frameworks have evolved beyond technical security guidance into strategic governance instruments that support Enterprise Risk Management (ERM). The findings indicate that both the NIST Cybersecurity Framework (CSF) 2.0

ISSN: 2971-7760 | VOL 6, ISS 3 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21770424
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

and ISO/IEC 27001:2022 contribute significantly to organizational resilience by strengthening governance structures, improving cyber risk visibility, supporting regulatory compliance, and facilitating informed decision-making. However, their contribution to ERM is achieved through different but complementary implementation philosophies.

A major finding of this study is that the introduction of the **Govern** function in NIST CSF 2.0 represents a significant advancement in cybersecurity governance. Earlier versions of the framework primarily emphasized operational cybersecurity activities, whereas Version 2.0 explicitly recognizes governance as the foundation for effective cyber risk management (NIST, 2024). This finding supports recent studies arguing that cybersecurity should be embedded within enterprise governance rather than managed solely by information technology departments (World Economic Forum, 2025; Quinn et al., 2024). By integrating cybersecurity governance with organizational strategy, NIST CSF 2.0 enables executive management to align cybersecurity investments with enterprise objectives, risk appetite, and long-term organizational resilience.

The study further reveals that ISO/IEC 27001:2022 remains one of the most comprehensive governance mechanisms for institutionalizing information security management. Through its Information Security Management System (ISMS), the standard promotes structured risk assessment, documented policies, internal audits, leadership accountability, and continual improvement. These characteristics enhance organizational consistency and provide external assurance through internationally recognized certification. The findings therefore corroborate previous research demonstrating that certified information security management systems improve governance maturity, stakeholder confidence, and regulatory compliance (ISO, 2022; ISACA, 2022).

Although both frameworks support Enterprise Risk Management, they exhibit distinct comparative advantages. NIST CSF 2.0 provides greater implementation flexibility and facilitates communication between technical specialists and executive decision-makers through a common risk language. Conversely, ISO/IEC 27001:2022 offers greater procedural discipline through documented management processes and measurable compliance requirements. These complementary characteristics suggest that organizations should avoid viewing the frameworks as substitutes. Instead, they should adopt an integrated governance strategy that combines the strategic adaptability of NIST CSF 2.0 with the operational rigor and certifiable management processes of ISO/IEC 27001:2022. Such integration is consistent with contemporary enterprise governance principles that advocate combining multiple governance instruments to address increasingly complex organizational risks (COSO, 2017; ISO, 2018).

The comparative findings also have important implications for organizational resilience. As cyber threats continue to evolve in

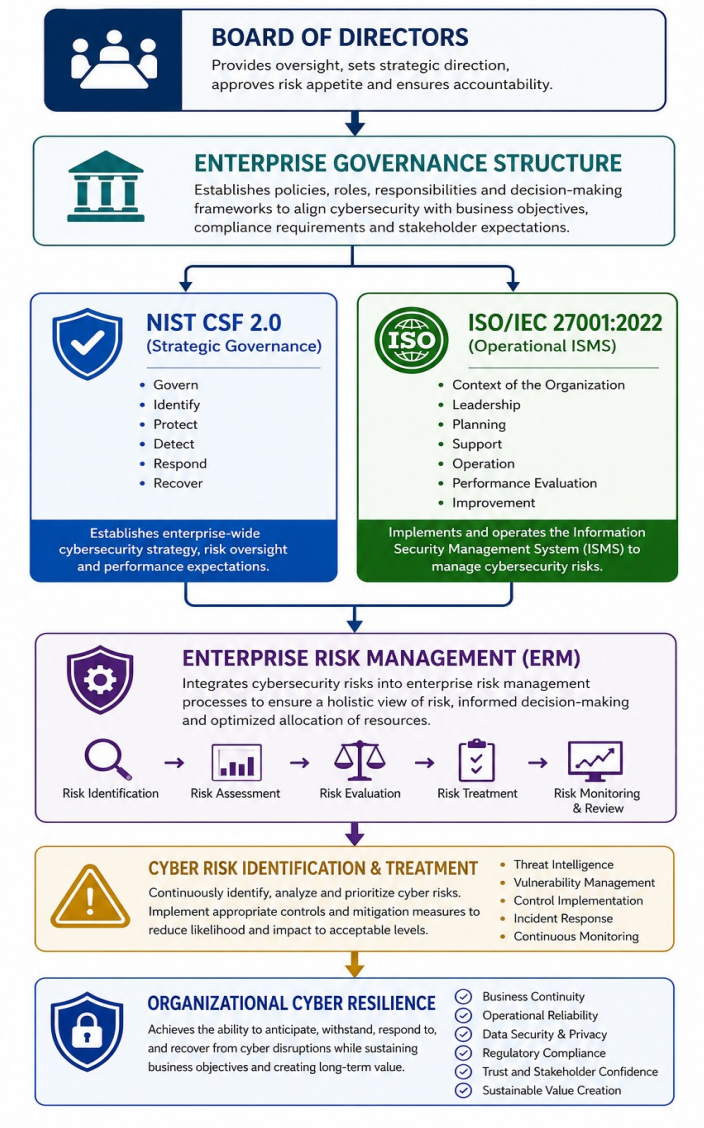
ISSN: 2971-7760 | VOL 6, ISS 3 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21770424
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

sophistication and frequency, organizations require governance frameworks capable of supporting continuous risk monitoring, rapid incident response, business continuity, and organizational learning. The combined implementation of NIST CSF 2.0 and ISO/IEC 27001:2022 provides a robust governance architecture that enhances cyber resilience by integrating strategic oversight, operational controls, performance monitoring, and continual improvement. This integrated approach enables organizations to respond more effectively to emerging cyber risks while protecting critical business processes and stakeholder interests.

From a managerial perspective, the findings emphasize the increasing responsibility of boards of directors, executive management, Chief Information Security Officers (CISOs), Chief Risk Officers (CROs), internal auditors, and compliance professionals in cybersecurity governance. Effective implementation of either framework requires leadership commitment, cross-functional collaboration, adequate resource allocation, and continuous organizational learning. Cybersecurity governance can no longer be regarded as the exclusive responsibility of information technology departments; rather, it has become a core element of enterprise governance requiring active oversight by senior management and governing boards.

The findings further suggest important implications for regulators and policymakers. Financial institutions, healthcare organizations, government agencies, educational institutions, and operators of critical national infrastructure increasingly operate within complex digital ecosystems characterized by interconnected technologies, cloud computing, artificial intelligence, and third-party service providers. Regulatory authorities should therefore encourage governance frameworks that integrate cybersecurity risk management with broader Enterprise Risk Management objectives while remaining adaptable to sector-specific operational requirements. Such an approach would strengthen organizational resilience, improve regulatory compliance, and contribute to national cybersecurity preparedness.

ISSN: 2971-7760 | VOL 6, ISS 3 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21770424
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA



ISSN: 2971-7760 | VOL 6, ISS 3 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21770424
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

Figure 4.1 Integrated Cybersecurity Governance Model for Enterprise Risk Management

Source: Developed by the Author (2026).

5. Conclusion and Recommendations

This study comparatively evaluated the NIST Cybersecurity Framework (CSF) 2.0 and ISO/IEC 27001:2022 with respect to their contribution to Enterprise Risk Management objectives. The analysis established that both frameworks play significant roles in strengthening cybersecurity governance, enhancing organizational resilience, supporting regulatory compliance, and improving enterprise-wide cyber risk management. Nevertheless, they differ in implementation philosophy, governance orientation, and operational application.

The study concludes that NIST CSF 2.0 provides superior strategic flexibility through its governance-oriented and risk-based approach, enabling organizations to align cybersecurity with enterprise objectives and executive decision-making. Conversely, ISO/IEC 27001:2022 provides a comprehensive Information Security Management System supported by standardized controls, documented procedures, continual improvement, and internationally recognized certification. These differences should not be interpreted as competitive alternatives but rather as complementary governance mechanisms capable of reinforcing one another when implemented in an integrated manner.

The principal contribution of this study lies in demonstrating that the integration of NIST CSF 2.0 and ISO/IEC 27001:2022 provides a more comprehensive foundation for Enterprise Risk Management than the adoption of either framework independently. Combining NIST's strategic

ISSN: 2971-7760 | VOL 6, ISS 3 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21770424
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

governance orientation with ISO/IEC 27001's structured management system enables organizations to strengthen cyber resilience, improve governance maturity, enhance regulatory compliance, and support sustainable organizational performance in increasingly complex digital environments.

Based on these findings, the study makes the following recommendations:

1. Organizations should adopt an integrated implementation strategy that combines NIST CSF 2.0 and ISO/IEC 27001:2022 to maximize strategic governance and operational effectiveness.
2. Boards of directors and executive management should formally embed cybersecurity governance within Enterprise Risk Management processes to ensure cyber risks are considered alongside strategic, financial, operational, legal, and reputational risks.
3. Organizations should invest in continuous cybersecurity training, governance maturity assessments, and regular reviews of cybersecurity performance to strengthen organizational resilience.
4. Regulatory authorities should encourage harmonized cybersecurity governance practices that recognize the complementary strengths of international cybersecurity frameworks while allowing flexibility for sector-specific implementation.
5. Future research should empirically evaluate the effectiveness of integrated NIST CSF 2.0 and ISO/IEC 27001:2022 implementation across different industries and organizational contexts, particularly within developing economies.

The growing complexity of cyber threats requires governance frameworks that extend beyond technical security controls toward enterprise-wide risk governance. Integrating NIST CSF 2.0 and ISO/IEC 27001:2022 within Enterprise Risk Management provides organizations with a practical and sustainable approach for strengthening cybersecurity governance, improving organizational resilience, and supporting long-term strategic success.

tetfund
TERTIARY EDUCATION TRUST FUND

References

AlHogail, A. (2021). Improving information security culture through cybersecurity governance: A conceptual framework. *Information & Computer Security, 29*(5), 817–835.

Angelini, M., Blasi, L., Lenti, S., Santucci, G., & Soldani, F. (2022). Integrating NIST and ISO/IEC 27001 for automated cyber risk assessment. *Computers & Security, 118*, 102726.

ISSN: 2971-7760 | VOL 6, ISS 3 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21770424
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

Bada, M., & Nurse, J. R. C. (2020). Developing cybersecurity education and awareness programmes for small and medium enterprises. *Information & Computer Security, 28*(4), 573–590.

Basel Committee on Banking Supervision. (2021). *Core principles for effective banking supervision*. Bank for International Settlements.

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

Deloitte. (2025). *Global future of cyber survey 2025*. Deloitte Insights.

ENISA. (2021). *Cybersecurity culture guidelines: Behavioural aspects of cybersecurity*. European Union Agency for Cybersecurity.

Gartner. (2025). *Top cybersecurity trends for 2025*. Gartner Research.

Hopkin, P. (2024). *Fundamentals of risk management: Understanding, evaluating and implementing effective risk management* (7th ed.). Kogan Page.

IBM Security. (2022). *Cost of a data breach report 2022*. IBM Corporation.

IBM Security. (2023). *Cost of a data breach report 2023*. IBM Corporation.

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

Information Systems Audit and Control Association. (2022). *State of cybersecurity 2022*. ISACA.

Information Systems Audit and Control Association. (2024). *State of cybersecurity 2024*. ISACA.

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

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

International Organization for Standardization. (2022). *ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection—Information security controls*. ISO.

Kure, H. I., Islam, S., & Mouratidis, H. (2021). Cybersecurity resilience: A review and future research directions. *Computers & Security, 102*, 102196.

ISSN: 2971-7760 | VOL 6, ISS 3 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21770424
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

McIntosh, T., Susnjak, T., Liu, T., Watters, P., & Ng, A. (2024). From protection to resilience: A comparative analysis of modern cybersecurity governance frameworks. *Computers & Security, 138*, 103663.

National Institute of Standards and Technology. (2024). *Cybersecurity framework (CSF) 2.0*. U.S. Department of Commerce.

National Institute of Standards and Technology. (2024). *Cybersecurity Framework 2.0: Enterprise Risk Management (ERM) quick-start guide*. U.S. Department of Commerce.

National Institute of Standards and Technology. (2024). *NIST Special Publication 800-37 Rev. 2: Risk management framework for information systems and organizations*. U.S. Department of Commerce.

National Institute of Standards and Technology. (2024). *NIST Special Publication 800-39: Managing information security risk*. U.S. Department of Commerce.

National Institute of Standards and Technology. (2024). *NIST Special Publication 800-53 Rev. 5: Security and privacy controls for information systems and organizations*. U.S. Department of Commerce.

National Institute of Standards and Technology. (2025). *Integrating cybersecurity and enterprise risk management (NIST IR 8286 series)*. U.S. Department of Commerce.

Quinn, S. D., McBride, M., & Boyens, J. (2024). *Cybersecurity Framework 2.0 enterprise risk management quick-start guide*. National Institute of Standards and Technology.

Rose, P. S., & Hudgins, S. C. (2021). *Bank management and financial services* (10th ed.). McGraw-Hill.

Safa, N. S., Maple, C., Watson, T., & Von Solms, R. (2020). Human aspects of information security in organisations: A review. *Journal of Information Security and Applications, 54*, 102565.

Stoltz, J. (2024). Risk management framework implementation and continuous cybersecurity monitoring: A systematic review. *Journal of Cybersecurity and Privacy, 4*(2), 311–329.

World Economic Forum. (2023). *Global cybersecurity outlook 2023*. World Economic Forum.

World Economic Forum. (2024). *Global cybersecurity outlook 2024*. World Economic Forum.

ISSN: 2971-7760 | VOL 6, ISS 3 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21770424
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

World Economic Forum. (2025). *Global cybersecurity outlook 2025*. World Economic Forum.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cybersecurity awareness, knowledge and behaviour: A comparative study across organisations. *Computers & Security, 109*, 102383.

Additional Foundational References

Aven, T. (2021). *Risk assessment and risk management: Review of recent advances*. Reliability Engineering & System Safety, *205*, 107291.

Bromiley, P., McShane, M., Nair, A., & Rustambekov, E. (2021). Enterprise risk management: Review, critique and research directions. *Long Range Planning, 54*(4), 102027.

Demirgüç-Kunt, A., Kane, E. J., & Laeven, L. (2008). *Deposit insurance around the world: Issues of design and implementation*. MIT Press.

ISACA. (2023). *COBIT 2019: Governance and management objectives*. ISACA.

Kaplan, R. S., & Mikes, A. (2021). Managing risks: A renewed framework for enterprise risk management. *Harvard Business Review, 99*(3), 48–57.

Mishkin, F. S. (2022). *The economics of money, banking, and financial markets* (13th ed.). Pearson.

NIST. (2024). *Cybersecurity Framework 2.0 reference tool*. National Institute of Standards and Technology.

Peltier, T. R. (2021). *Information security policies, procedures, and standards: Guidelines for effective information security management*. Auerbach Publications.

Whitman, M. E., & Mattord, H. J. (2022). *Principles of information security* (7th ed.). Cengage Learning.

Von Solms, B., & Van Niekerk, J. (2021). From information security to cybersecurity. *Computers & Security, 97*, 101944.