ISSN (Print): 1060-6076
ISSN (Online): Applied

The Journal of African Development
2026; Vol 7: Issue 1
https://www.afea-jad.com/

Risk Management in Relation to Cyber Security and How it is Applied in the Modern Organization.

Dr Deepak Saxena[1], Dr. Megha Gupta[2], Dr. Rahul Kumar Sharma[3], Mr. Chandrapal Singh Arya[4], Varun Bharadwaj[5]

[1] Integrated Academy of Management and Technology, Ghaziabad, India.
Email: deepak.saxena73@gmail.com
[2] Noida Institute of Engineering and Technology, Greater Noida, India.
Email: meghagupta.cse@niet.co.in
[3] Noida Institute of Engineering and Technology, Greater Noida, India.
Email: rahulsharma.cse@niet.co.in
[4] Noida Institute of Engineering and Technology, Greater Noida, India.
Email: aryanchandrapal@gmail.com
[5] I.P.(P.G.) College Campus 2, Bulandshahr, India.
Email: varunrocking1990@gmail.com
Corresponding Author:
Mr. Chandrapal Singh Arya[4]
Email: aryanchandrapal@gmail.com.

Cite This Paper as: Dr Deepak Saxena, Dr. Megha Gupta, Dr. Rahul Kumar Sharma, Mr. Chandrapal Singh Arya, Varun Bharadwaj (2026) Risk Management in Relation to Cyber Security and How it is Applied in the Modern Organization..The Journal of African Development l, Vol.7, No.1, 1096-1103

KEYWORDS

cybersecurity risk management, artificial intelligence, zero trust architecture, cyber resilience, post-quantum cryptography, NIST CSF, ISO 27001, risk quantification.

ABSTRACT

Current cybersecurity risk management approaches fail to adequately address today's organizational resilience needs due to the increasing complexity of cyber threats driven by the rise of artificial intelligence (AI) and the imminent arrival of quantum computing. The current paper critically reviews the latest risk management strategies for cybersecurity, comparing compliance-centric methods with adaptive, AI-supported, and quantum-resistant solutions. We assess the effectiveness of integrated risk management architectures, zero trust and cyber resilience frameworks and evaluate how they have evolved in recent years, in line with recent developments, such as NIST SP 800-37 Rev. 2 (2025), ISO/IEC 27001:2025 and new threat detection systems powered by AI. The study marks a paradigm shift in three areas: continuous risk assessment, automated response orchestration and preparedness for post-quantum cryptographic protocols. The results show that companies with a hybrid human-AI governance model and real-time risk quantification methods and companies that have implemented proactive quantum-safe transition planning have measurably better security postures. The paper concludes with a strategic roadmap for enterprise adaptive cybersecurity risk management with a focus on the intersection of technology, culture and regulation.

1. INTRODUCTION

The modern organizational environment is operating in a more and more threatening digital world. Cybersecurity incidents have evolved from mere technical nuisances to existential threats that can lead to organizational collapse, regulatory penalties and reputational annihilation. By 2025, the global cost of cybercrime will surpass $10.5 trillion per annum, which is one of the greatest wealth transfers in history of mankind (Morgan, 2020). The threat landscape in modern organisations is not symmetric, as adversary actors, from state-sponsored to criminal syndicates and insider threats, use ever more advanced tools and methods such as Generative AI, automated attack frameworks or quantum cryptanalysis. Cybersecurity risk management has historically been done in a reactive way, with periodic compliance audits, checklists, and incident response. But with the pace at which threats are evolving today, such approaches are structurally unsound. Cloud, remote working architectures, an exploding Internet of Things (IoT) and the supply chain digitization have dramatically increased the attack surface. At the same time, the landscape of regulations has become stricter worldwide, such as the NIS2 Directive from the European Union, which introduces new cybersecurity accountability obligations for organizational management ....

(European Parliament, 2022), and sector-specific regulations in the U.S. Securities and Exchange Commission (SEC) that have established cybersecurity disclosure requirements (U.S. Securities and Exchange Commission, 2023). It looks at how cybersecurity risk management has developed, current practices, and the future. From a compliance-led to an intelligence-led approach.

AI-powered, zero trust and quantum-resistant risk ecosystems. The goal is to conduct a broad and deep scholarly examination of successful approaches to risk management, including highlights of the significant success factors, long-term issues, and organizational priorities for effective cybersecurity governance. The theoretical foundations and conceptual framework were examined.Theoretical foundations and conceptual framework were explored.

Consequences of Risk and the need for Mitigation Strategies.

Risk Management in Cybersecurity Context

The discipline is based on classical risk theory, but it has been adjusted to the specific nature of the digital environment; threats constantly evolve, defenders and attackers have conflicting information, there are interdependencies, and information assets are intangible (Siponen & Oinas-Kukkonen, 2007). This principle of risk in cyber security is still as follows: Risk = Threat × Vulnerability × Impact. This formulation, however, has come to be more dynamic and takes into consideration temporal aspects, control effectiveness, and residual risk acceptance. Modern concepts focus on the dynamic nature of risk and consider it as a condition that needs to be continuously managed within an organization's risk appetite (Stoneburner et al., 2002).

Evolution of Cybersecurity Risk Management Paradigms

Let's look at the cybersecurity risk management evolution, which can be imagined in three paradigmatic phases: Compliance-centric (1990s–2010s): Compliance with prescriptive standards (ISO 27001, COBIT, PCI DSS) via audit and control checklists (check the box). The focus of risk management was mainly on compliance in the past, not on resilience in the future. Threat Centric Era (2010s-2020s): Intelligence based defense, threat modelling and indicator based detection. There was investment in Security Operations Centers (SOCs), threat intelligence solutions and incident response. The risk management function became more dynamic, but still largely reactive. Resilience-Centric Era (2020s to present): The assumption of breach will be accompanied by continuous adaptation and integrated business continuity. Organizations understand that the prevention is the only option but draw attention to the reduction of mean time to detect (MTD), mean time to respond (MTR), and business impact while maintaining operational continuity (Linkov et al., 2018).

Conceptual Framework: The Adaptive Cybersecurity Risk Management Model

In this paper, we introduce a novel conceptual framework, called Adaptive Cybersecurity Risk Management Model (ACRMM), which combines current approaches into four interlocking dimensions: 1. Governance Architecture: Organizational structures, accountability mechanisms and board-level oversight 2. Technical Controls: Zero trust architectures, AI and machine learning-based detection, encryption and access management 3. Operational Processes: Continuous monitoring, automated response and incident management 4. The following discussion on specific risk management strategies is based on this framework of Strategic Adaptation: Quantum preparedness, supply chain resilience, and regulatory anticipation.

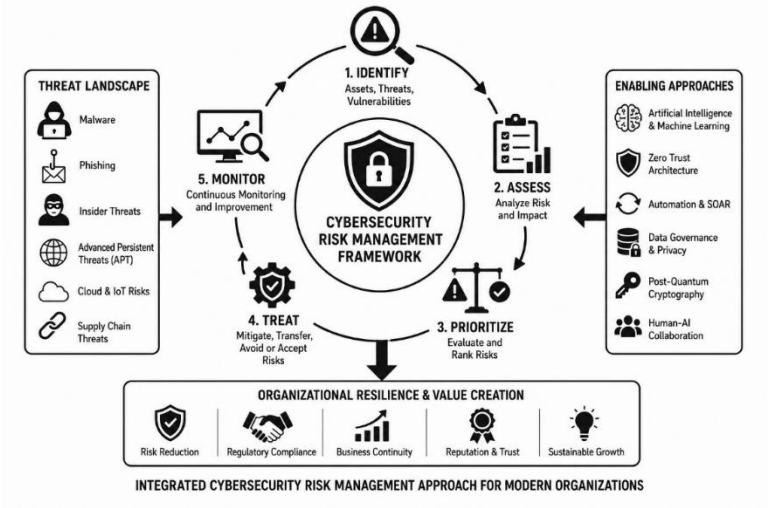

Figure 1: Integrated Cybersecurity Risk Management Approach for Modern Organizations

Figure 1 illustrates the integrated cybersecurity risk management lifecycle, highlighting the relationship between threat landscapes, enabling technologies, and organizational resilience outcomes."

Contemporary Risk Management Frameworks and Standards

NIST Cybersecurity Framework 2.0 and Risk Management Integration

The recent NIST Cybersecurity Framework (CSF) 2.0 published in February 2024 is a major update to the guidance on risk management. Unlike the previous version, CSF 2.0 has a dedicated governance pillar, labeled as GOVERN, which explicitly includes governance as one of the key functions of the CSIRM. NIST (2024) raises cybersecurity risk management to an enterprise-level accountability mechanism. The six functions of the framework – Govern, Identify, Protect, Detect, Respond, Recover – give a comprehensive lifecycle perspective to risk management. The GOVERN function is designed to focus on the organization's risk management strategy, the internal roles and responsibilities, and the integration of management of cyber risk with the enterprise's risk management (ERM) process. This integration is important because cybersecurity risk can't be addressed without considering financial, operational, and reputational risks (NIST, 2024). NIST SP 800-37 Rev. 2 is the operational methodology for the implementation of CSF principles. It focuses on near real-time risk management via continuous monitoring, automated control evaluation and authorization (NIST, 2025). It's a shift from the typical 3-year authorization cycles to ongoing risk acceptance decisions as informed by the latest threat intelligence and control effectiveness.

ISO/IEC 27001:2025 and Risk-Based Information Security

The ISO/IEC 27001 standard, which was last updated in 2025, continues to have a risk-based approach to information security management systems (ISMS). The revision in 2025 highlights a focus on more flexibility in assessing risk approaches, better business process integration and added support for new technologies such as AI and cloud services (ISO/IEC, 2025). The ISO 27001:2025 standard presents a risk management maturity plan-action-check-act (PACA) cycle to provide a structured methodology for improving the maturity of their risk management: • Plan: Establish and document risk assessment criteria, identify risks, and select appropriate controls from Annex A; • Do: Implement and operate the controls; • Check: Monitor and review control effectiveness against risk treatment objectives; • Act: Maintain and improve the ISMS based on review outcomes. Critically, ISO 27001:2025 requires that organizations demonstrate continuous improvement in the maturity of risk management, rather than a state of compliance – aligned with the risk management paradigm of resilience (ISO/IEC, 2025).

FAIR Model: Quantitative Risk Analysis

The Factor Analysis of Information Risk (FAIR) model offers a quantitative approach to cybersecurity risk analysis that enables risks to be expressed in financial terms that are easily understood by organizational management. There are recent examples of the use of FAIR in enterprise environments to support investment decisions, negotiate insurance premiums, and communicate risk to the board (Jones, 2020). As mentioned the effectiveness of the model requires good quality data inputs, and this is hard to come by for new threat categories and zero day vulnerabilities.

AI-Driven Risk Management Approaches

Machine Learning for Threat Detection and Risk Assessment

The use of artificial intelligence (AI) in the field of cybersecurity risk management has revolutionized the industry. In today's world of machine learning (ML) algorithms, huge amounts of data are collected from telemetry to detect any irregular patterns that might signal malicious activity. Unlike signature-based detection, ML methods can detect new attacks that haven't yet been seen in the wild, as long as they aren't explicitly included in the training examples. (Buczak & Guven, 2016) Current AI-based risk management solutions leverage multiple ML paradigms such as: Supervised Learning: Learn from labeled datasets of previous patterns of attacks to then categorize incoming attacks. For known malware families, variants of them and intrusion signatures. Unsupervised Learning: Learns deviations from known behavior without labelled training examples. Advanced persistent threats (APTs), zero-day exploits and insider threats are detected. Reinforcement Learning: Allows for automated response systems that learn optimal mitigation actions based on the environment's feedback, and is being used more and more in automated incident response orchestration. The use of AI in risk management is not limited to the detection phase; it also has a predictive component known as predictive risk assessment. Today, organizations use AI to predict when vulnerabilities are likely to be exploited, and how much time they have for exposure and to apply patches – prioritizing them by critical business and by threat dynamics (SANS Institute, 2025).

Generative AI and Emerging Risk Dimensions

Generative AI has two sides to its implications for cybersecurity risk management. Generative AI is not just a tool for defense, it's a force to be reckoned with for the attackers as well; it has automated code review, it can generate synthetic data for training, and it can simulate phishing attacks intelligently. AI-powered deepfakes enable social engineering, AI can aid in the automated discovery of vulnerabilities to exploit, and AI can create polymorphic malware that is more difficult for traditional security measures to detect (CISA, 2025). The NIST AI Risk Management Framework (AI RMF 1.0) offers basic principles but rapid advancements in technology makes it important to continually adapt the framework (NIST, 2023)..

Automated Risk Response Orchestration

Cyber attacks are so fast that the human response can not keep up. So-called Security Orchestration, Automation, and Response (SOAR) systems can automatically respond to specific threat categories in real time with mitigation action, without requiring human intervention. These systems combine threat intelligence, SIEM alerts and vulnerability information to trigger predefined playbooks; isolate endpoints that are compromised, revoke credentials, block IPs that are malicious and escalate to human analysts for novel threats (Gartner, 2024). Automated response poses new risks, however: false-positive disruption, cascading failures and adversarial manipulation of automated decision pathways. Robust human-in-the-loop governance is needed for high impact decisions and to ensure automated logic is continually validated.

Zero Trust Architecture and Risk Reduction

Principles of Zero Trust

Zero Trust Architecture (ZTA) is a shift in thinking of network security that follows the mantra "never trust, always verify. Instead of relying on an implicit assumption about the integrity of network traffic, Zero Trust makes no such assumption and verifies every access attempt, regardless of its origin (Rose et al., 2020). For risk management, Zero Trust offers granular visibility into access patterns, minimises opportunities for lateral movement in the event of successful access and allows precise risk quantification, using identity-centric metrics instead of assuming the topology of the network.

Implementation Challenges and Risk Trade-offs

Implementing Zero Trust offers many benefits for organizations, but also comes with significant risks, including operational disruption, complexity management, and supply chain integration risks. Risk management in Zero Trust adoption means phasing the implementation while monitoring the business impact metrics along with security effectiveness metrics. While security is important, the level of restrictions and security rigor needs to be balanced against operational continuity, as too much restriction may lead to proliferation of shadow IT and circumvention behaviors, which will increase the over all risk(Rose etal., 2020).

Cyber Resilience and Business Continuity Integration

Beyond Prevention: The Resilience Imperative

Modern risk management understands that total risk elimination is impossible with determined forces. Nowadays, Cyber resilience – the capacity to anticipate, withstand, recover from, and adapt to cyber attacks – is the overall goal (Linkov et al., 2018). This view combines the concepts of business continuity planning, crisis management, and organizational adaptation with cybersecurity risk management. The resilience approach focuses on the following: • Anticipation – threat intelligence, scenario planning, red team exercises; • Withstanding – powerful architectures, redundant systems, and quick detection; • Recovery – backup integrity, incident response capabilities, and communication protocols; • Adaptation – post incident learning, control enhancement, strategic adjustment.

Regulatory Drivers of Resilience

Resilience capabilities are increasingly being required by regulatory frameworks. It is also expected that organisations are able to demonstrate resilience testing, recovery time objectives and board-level accountability for cyber incidents, as stipulated by the EU's Digital Operational Resilience Act for financial entities (European Commission, 2020) and the UK's Operational Resilience Framework (UK) (UK Securities and Exchange Commission, 2023). These guidelines will make resilience a requirement and not an aspiration and have severe consequences when there is not enough preparation. The need for regulatory resilience requirements is now a requirement to be incorporated into risk management frameworks, encompassing both technical capability and governance documentation and audit trails.

Quantum Computing and Post-Quantum Risk Management

The Quantum Threat to Current Cryptography

Today's cryptographic systems are at risk of being compromised by quantum computing. It is possible to factor a large integer in polynomial time on a quantum computer using Shor's algorithm, which makes both RSA and Diffie-Hellman

and elliptic curve cryptography vulnerable (Bernstein & Lange, 2017). Symmetric key security margins are halved with Grover's algorithm for unstructured search. The timing of the arrival of quantum computers with cryptographic relevance is still far-fetched (anywhere from five to twenty years) and the implications for risk management are immediate. Potential opponents are already doing "harvest now, decrypt later" attacks, gathering encrypted information for the future, when quantum computers will be available. There is special urgency for organizations that have a long data lifecycle requirement (such as healthcare, government, critical infrastructure).

Post-Quantum Cryptographic Transition

After evaluating algorithms for several years, NIST has set out to standardize post-quantum cryptographic (PQC) algorithms. The algorithms chosen (CRYSTALS-Kyber for key encapsulation, CRYSTALS-Dilithium, FALCON, and SPHINCS+ for digital signatures) are secure against known quantum attacks (NIST, 2024). Risk management for PQC transition involves: • Cryptographic Inventory: Comprehensive mapping of algorithm usage across systems, applications, and third-party services • Vulnerability Assessment: Identification of high-risk data and communication flows requiring priority migration • Hybrid Deployment: Concurrent operation of classical and PQC algorithms during transition periods • Performance Optimization: Addressing computational overhead and bandwidth impacts of PQC algorithms The transition timeline is constrained by hardware limitations, interoperability requirements, and the complexity of updating legacy systems. Rather than making an attempt to migrate everything at once, risk managers need to prioritize according to data sensitivity, exposure time, and regulatory requirements.

Supply Chain Risk Management

The Supply Chain Attack Surface

Organizations today have an enormous attack surface to manage, and a reliance on third party vendors, open source components, and cloud service can make it even larger. The SolarWinds compromise (2020), the Log4j vulnerability (2021) and the Log4Libk compromise (2021) are examples of attacks that seek to exploit more vulnerable components in the supply chain to attack less vulnerable ones further downstream (ENISA, 2021). Supply chain risk management needs: • Vendor Assessment: Security maturity assessment, contractual security requirements, continuous monitoring • Software Composition Analysis: Identification and tracking of open-source or commercial components for vulnerabilities • Secure Development Practices: Integration of security into vendor's development lifecycle • Incident Coordination: Defined communication and response protocols for supply chain compromise.

Software Bills of Materials (SBOM)

The U.S. Executive Order on Improving the Nation's Cybersecurity (2021) called for SBOMs in federal software acquisitions, which helped to drive adoption. SBOMs can be machine-readable lists of software components that can be used for automated vulnerability correlation and risk assessment (NTIA, 2021). SBOM adoption is key to supply chain risk management today and must be incorporated into procurement workflows, vulnerability management systems and incident response processes.

Organizational Governance and Human Factors

Board-Level Accountability

Thanks to regulatory requirements, shareholder demands, and high-profile cyber breaches, cybersecurity risk management has become a priority for boards of directors. Public companies are required to report on cyber security expertise on their boards and management's role in assessing and managing risks under the U.S. Securities and Exchange Commission's rules, along with material incidents within 4 business days (U.S. Securities and Exchange Commission, 2023). Effective governance requires: Board Cybersecurity Literacy: Adequate technical knowledge to support the board's role; Risk Appetite Definition: Explicit statement of acceptable risk and resource levels; Performance Metrics: Use meaningful key risk indicators (KRIs) and key performance indicators (KPIs); Crisis Authority: Having the right escalation procedures and decision making authority when an incident occurs.

Security Culture and Human Risk

Hacks and security incidents are still caused primarily by human factors despite technological advances. Phishing, social engineering, and insider threats are based on psychological weaknesses, not technical. Organizations with a mature security culture, where security is seen as a facilitator to, not a hindrance to, secure behaviors, have measurably lower incident rates and quicker response times, according to research (Siponen & Oinas-Kukkonen, 2007).

Emerging Trends and Future Directions

Continuous Risk Assessment and Dynamic Authorization

Cybersecurity risk management is the new game of continuous, automated assessment of risk. Dynamic authorization

systems are real-time risk-scoring, which can take into account data related to user behavior, device posture, threat intelligence, and geolocation to adjust access privileges. This method is called Zero Trust Network Access (ZTNA) or Software-Defined Perimeter (SDP) and allows for risk-oriented security based on changing contexts (Gartner, 2024).

Extended Detection and Response (XDR)

XDR platforms combine detection and responses for endpoints, networks, cloud services, and identity into a single workflow. XDR can correlate events across different security domains, which have historically lived in silos, to help improve the accuracy of threat detection and ease analyst workload. The advantages of risk management are that it provides all-encompassing visibility, automated triage, and integrated response orchestration.

Regulatory Harmonization and Global Standards

Cybersecurity rules are spread out among jurisdictions, which can cause complexity and potential gaps in compliance. New regulatory harmonization initiatives, such as the EU Cyber Resilience Act, international standards harmonization and sector-specific regulations, look forward to greater uniformity in risk management standards. Organizations need to get ready for convergence of regulations and remain flexible to local government requirements.

Discussion and Critical Analysis

Framework Integration Challenges

With the plethora of risk management frameworks like NIST CSF, ISO 27001, COBIT, FAIR, CIS Controls, organizations face the challenge of integrating these. Although each of the above has its merits, there can also be duplication, ambiguity, and demands on resources when they are all used concurrently. Thoughtful framework selection – instead of uncritical adoption of several standards – is key to effective risk management, which depends on the organizational context, regulatory requirements and maturity.

The AI-Risk Paradox

The challenge with AI for cybersecurity risk management is a fundamental paradox: it strengthens defenders' tools while simultaneously empowering the attackers' arsenal. The complexity of governance needs arises from the organizations needing to manage risk with their own AI deployments and make use of AI as a defense mechanism. Given the rapid rate of change for AI, we need adaptable governance structures that respond to it, as traditional governance cycles cannot keep up.

Resource Constraints and Risk Prioritization

Cybersecurity risk management operates within resource constraints that necessitate prioritization. However, risk prioritization methodologies often lack rigor, relying on subjective assessments rather than quantitative analysis. The integration of FAIR-style quantification with continuous monitoring data offers promise for more objective resource allocation, though data quality and model limitations remain significant challenges.

The Human-AI Collaboration Imperative

Cybersecurity risk management takes place in a resource-limited environment requiring prioritization. But there are issues with risk prioritisation methodologies, as they do not always have rigor, rather they are based on subjective assessment than quantitative analysis. Combining FAIR quantification with continuous monitoring data has the potential for more objective resource allocation, but data quality and model limitations remain a challenge.

Risk Management Approach	**Key Technologies Used**	**Major Benefits**	**Primary Challenges**	**Future Relevance**
Traditional Compliance-Based Security	Firewalls, Antivirus, Audit Checklists	Regulatory compliance, basic protection	Reactive approach, limited adaptability	Low
AI-Driven Threat Detection	Machine Learning, Behavioral Analytics	Real-time anomaly detection, predictive analysis	False positives, AI manipulation risks	Very High
Zero Trust Architecture (ZTA)	Identity Management, MFA, Micro-Segmentation	Reduced lateral movement, strong access control	Complex implementation, legacy compatibility	Very High
Cyber Resilience Framework	Backup Systems, Incident Response, Recovery	Faster recovery and business continuity	High operational cost	High

Risk Management Approach	Key Technologies Used	Major Benefits	Primary Challenges	Future Relevance
	Planning			
Quantitative Risk Analysis (FAIR Model)	Risk Scoring, Financial Modeling	Better investment decisions, measurable risk	Requires accurate data	High
Post-Quantum Cryptography (PQC)	Quantum-Resistant Algorithms	Future-proof encryption security	Migration complexity, performance overhead	Critical
Supply Chain Risk Management	SBOM, Vendor Security Assessment	Improved third-party security visibility	Dependency on vendor transparency	High
Automated SOAR Platforms	Security Automation, AI Orchestration	Rapid incident response, reduced workload	Automation errors, overdependence	Very High

Table 1: Comparative Analysis of Contemporary Cybersecurity Risk Management Approaches

CONCLUSION AND RECOMMENDATIONS

Modern organizations have moved beyond compliance-driven check-the-box cybersecurity risk management to become intelligence-driven, enterprise-governance-and-business-driven disciplines. A few of the hallmarks of the modern risk management environment are the incorporation of artificial intelligence, zero trust frameworks, quantum readiness, and resilience-focused goals. The following strategic recommendations are provided to organizational leaders and risk management practitioners from this paper: 1. Implement Continuous Risk Management: Implement continuous monitoring, automated control validation, and adaptive risk acceptance process in accordance to NIST SP 800-37 Rev. 2 principles instead of periodic assessments. 2. Use AI Wisely: Implement AI in threat detection, risk assessment, and response actions, but continue to include human actors in high-stakes decisions and for new classes of threats. 3. Implement Zero Trust Architectures: Step towards identity-centric and least-privilege-based architectures with an explicit verification of any access request. 4. Get ready for Quantum Transition: Start cryptographic inventory, target highly sensitive, long-lifecycle data for PQC adoption, and track NIST standardization progress. 5. Improve Supply Chain Visibility: Enable SBOM consumption capabilities, define vendor security requirements, and incorporate supply chain risk into enterprise risk management. 6. Shape and build Security Culture: Spend money on ongoing Security Awareness; design usable Security Controls; make Security a business facilitator, not a business hindrance. 7. Everyone should ensure that there's a clear cybersecurity governance structure, there's some real metrics for the board, and that there's a crisis authority for any material incident. The future of cybersecurity risk management is not about one technology or one single framework—it's about how these technological capabilities, organizational governance, and human expertise are adapted and integrated together. The ones that successfully integrate their cybersecurity risk management into the business, rather than treating as a technical compliance role will be better equipped to deal with a continuously changing threat landscape and take advantage of the opportunities given by digital transformation..

References

1. Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. Nature, 549(7671), 188–194. https://doi.org/10.1038/nature23461
2. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502
3. Cybersecurity and Infrastructure Security Agency. (2025). AI cybersecurity challenges and mitigation strategies. U.S. Department of Homeland Security. https://www.cisa.gov
4. ENISA. (2021). Threat landscape for supply chain attacks. European Union Agency for Cybersecurity. https://www.enisa.europa.eu
5. European Commission. (2020). Digital Operational Resilience Act (DORA): Proposal for a regulation.
6. European Commission. https://ec.europa.eu
7. European Parliament. (2022). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across

the Union (NIS2 Directive). Official Journal of the European Union. https://eur-lex.europa.eu

8. Gartner. (2024). Market guide for extended detection and response. Gartner Research. https://www.gartner.com
9. ISO/IEC. (2025). ISO/IEC 27001:2025 Information security, cybersecurity and privacy protection—Information security management systems—Requirements. International Organization for Standardization.
10. Jones, J. (2020). Measuring and managing information risk: A FAIR approach. Routledge.
11. Linkov, I., Trump, B. D., Pescaroli, G., & Florin, M. V. (2018). Resilience in the context of nuclear security.
12. Journal of Nuclear Materials Management, 46(3), 4–11.
13. Morgan, S. (2020). Cybercrime to cost the world $10.5 trillion annually by 2025. Cybersecurity Ventures. https://cybersecurityventures.com
14. National Institute of Standards and Technology. (2023). Artificial intelligence risk management framework (AI RMF 1.0). U.S. Department of Commerce. https://doi.org/10.6028/NIST.AI.100-1
15. National Institute of Standards and Technology. (2024). Cybersecurity framework 2.0. U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29
16. National Institute of Standards and Technology. (2024). Module-lattice-based key-encapsulation mechanism standard. Federal Information Processing Standards Publication 203. U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.203
17. National Institute of Standards and Technology. (2025). Risk management framework for information systems and organizations: A system life cycle approach for security and privacy (SP 800-37 Rev. 2). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-37r2
18. National Telecommunications and Information Administration. (2021). The minimum elements for a software bill of materials (SBOM). U.S. Department of Commerce. https://www.ntia.gov
19. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture (NIST SP 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207
20. SANS Institute. (2025). AI in cybersecurity: Threat detection and risk management applications. SANS Reading Room. https://www.sans.org
21. Siponen, M., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. ACM SIGMIS Database, 38(1), 60–80. https://doi.org/10.1145/1232310.1232317
22. Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems (NIST SP 800-30). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-30
23. U.S. Securities and Exchange Commission. (2023). Cybersecurity risk management, strategy, governance, and incident disclosure. Final Rule 33-11216. Federal Register. https://www.sec.gov