Beyond Compliance: A Risk-Based Approach to Cybersecurity Management

Ngsnet Hawarya

Saint Mary’s University of Minnesota

CYBR 615: Cybersecurity Change Management

Instructor: Scott McCoy

December 21, 2025

Beyond Compliance: A Risk-Based Approach to Cybersecurity Management

Cybersecurity has become a major concern for organizations as digital systems continue to support nearly every aspect of business operations. Data storage, communication platforms, financial transactions, and operational technologies are now deeply interconnected, which increases both efficiency and exposure to cyber threats. As a result, many organizations have turned to regulatory compliance frameworks as a primary way to manage cybersecurity risks. Standards such as NIST, ISO, and sector-specific regulations provide structured guidance and establish baseline security expectations. While these frameworks are important, relying on compliance alone has proven insufficient for addressing the evolving and unpredictable nature of cyber threats.

Compliance-driven cybersecurity often focuses on meeting required controls, passing audits, and demonstrating adherence to regulations. However, compliance does not necessarily reflect an organization’s actual risk exposure or its ability to respond effectively to emerging threats. Several studies suggest that organizations can remain compliant while still experiencing significant security incidents, showing a gap between regulatory compliance and real-world security outcomes (Sulaiman et al., 2022; Trinity & Sharma, 2023). This gap raises important questions about how cybersecurity should be managed in modern organizations.

A risk-based approach to cybersecurity management shifts the focus away from checklist compliance toward understanding and prioritizing real risks that directly threaten organizational objectives. Risk management considers not only technical vulnerabilities but also business context, asset value, threat likelihood, and potential impact. By integrating cybersecurity into broader enterprise risk management (ERM) processes, organizations can align security decisions with business strategy and adapt more effectively to change (Stine et al., 2020). This paper argues that although compliance frameworks provide a necessary foundation, cybersecurity management must move beyond compliance and adopt a risk-based approach to address the complexity of today’s digital environment.

Traditional IT Security and Compliance-Based Approaches

Traditional IT security models have historically focused on perimeter defense, technical controls, and standardized security practices. Firewalls, intrusion detection systems, access controls, and antivirus software were commonly implemented to protect organizational systems. Over time, as cyber threats increased and regulations expanded, compliance became closely tied to how organizations measured security effectiveness. Passing audits and demonstrating adherence to regulatory requirements became common measures of cybersecurity maturity.

Compliance frameworks play an important role by setting minimum standards across industries. Frameworks such as ISO/IEC 27001 and NIST security controls provide structured guidance for implementing security practices. According to Taherdoost (2022), these standards help organizations formalize security policies, define responsibilities, and create repeatable processes. From a management perspective, compliance offers assurance to regulators, customers, and stakeholders that basic security expectations are being met.

Despite these benefits, Compliance-driven security often focuses more on documentation and controls than on reducing real risk. Audits typically assess whether controls exist rather than whether they are effective in a specific organizational context. Joshi and Singh (2017) note that traditional security approaches frequently overlook contextual factors such as organizational culture, asset criticality, and threat dynamics. As a result, security efforts often become reactive rather than proactive, focusing on satisfying external requirements rather than proactively managing risk.

Another limitation of traditional security models is their tendency to treat all assets and threats similarly. Compliance frameworks often apply uniform controls across systems without fully accounting for differences in risk exposure. This approach can lead to inefficient allocation of resources, where low-risk systems receive the same level of attention as high-risk assets. Over time, this imbalance can reduce an organization's ability to respond to emerging threats and adapt to changing business conditions.

Compliance Versus Security: Understanding the Gap

The assumption that compliance equates to security is one of the ongoing challenges in cybersecurity management. While compliance establishes a baseline, it does not guarantee protection against advanced or evolving threats. Research shows that organizations may remain compliant while experiencing security breaches, particularly when threats fall outside the scope of regulatory controls (Trinity & Sharma, 2023).

Human factors play a significant role in security failures. Employees may bypass security policies for convenience, misunderstand procedures, or intentionally violate rules despite formal compliance structures. These behaviors are often not captured in compliance audits, which focus more on policy existence than real-world practice. As a result, organizations may appear secure on paper while remaining vulnerable in practice.

Another challenge is that compliance frameworks tend to lag the threat landscape. Regulations are updated periodically, but cyber threats evolve rapidly. Cremer (2022) emphasizes that data availability and threat intelligence gaps make it difficult for compliance-based approaches to address emerging risks effectively. Attack techniques such as zero-day exploits and social engineering campaigns often exploit weaknesses that are not explicitly addressed in regulatory controls.

Additionally, compliance-driven security can create a false sense of security. When organizations focus primarily on passing audits, cybersecurity may be viewed as a box-checking exercise rather than an ongoing risk management process. This mindset can limit critical thinking and discourage proactive security planning. Over time, the gap between compliance and actual security readiness becomes increasingly evident. One reason compliance continues to dominate cybersecurity practices is that it provides organizations with a sense of structure and certainty. Compliance frameworks offer clear rules, defined controls, and measurable outcomes, such as audit results or certification status. From a management perspective, this clarity simplifies decision-making and accountability. Executives can demonstrate that required steps were taken, even if those steps do not fully address the organization’s most critical risks.

Risk management, by contrast, introduces ambiguity that many organizations find uncomfortable. Assessing risk requires judgment, interpretation, and continuous reassessment, all of which involve uncertainty. Unlike compliance audits, risk assessments do not produce a simple pass or fail outcome. Instead, they highlight trade-offs between cost, usability, and protection. As a result, organizations may default to compliance because it feels safer and more defensible, even when it does not meaningfully reduce exposure to cyber threats (Sulaiman et al., 2022).

Another challenge lies in how responsibility for cybersecurity is distributed within organizations. Compliance activities are often assigned to specific teams or roles, such as compliance officers or auditors, which can unintentionally isolate cybersecurity from broader business decision-making. When security is treated as a compliance function rather than a risk management discipline, it may become disconnected from operational realities. Trinity and Sharma (2023) note that regulatory requirements often focus on minimum standards, which may not reflect the actual threat environment facing an organization. This disconnect can lead to security strategies that are technically compliant but strategically weak.

The reliance on compliance can also discourage proactive security improvements. Once an organization meets regulatory requirements, there may be little incentive to invest additional effort into addressing emerging risks that fall outside audit scope. Cremer (2022) emphasizes that cyber threats evolve faster than regulatory frameworks, leaving compliant organizations vulnerable to novel attack methods. In this context, compliance can unintentionally act as a ceiling rather than a foundation for cybersecurity practices.

Recognizing the gap between compliance and security is a critical step toward improving cybersecurity management. Compliance should be viewed as a baseline that supports risk management, not as a substitute for it. By reframing cybersecurity as a risk-driven process rather than a regulatory obligation, organizations can move toward more adaptive and effective security strategies that align with both operational needs and business objectives.

Risk-Based Cybersecurity Management Frameworks

One major advantage of a risk-based approach to cybersecurity management is its ability to support informed decision-making across different organizational levels. Unlike compliance-driven models, which often emphasize uniform control implementation, risk-based decision-making allows organizations to prioritize security investments based on their potential impact. This approach acknowledges that not all systems, data, or processes carry equal importance, and therefore should not receive identical levels of protection.

Risk-based prioritization requires organizations to evaluate cybersecurity risks in terms that leadership can understand, such as operational disruption, financial loss, legal exposure, and reputational damage. By translating technical risks into business outcomes, cybersecurity teams can more effectively communicate concerns to executives and board members. Stine et al. (2020) emphasize that integrating cybersecurity risk into enterprise risk discussions improves transparency and accountability, particularly when leadership must balance security needs with budgetary and operational constraints.

A critical element of risk-based decision-making is the concept of risk appetite. Organizations differ in their tolerance for risk based on industry, regulatory environment, and strategic objectives. A financial institution, for example, may have a lower tolerance for data breaches than a small technology startup. Risk-based cybersecurity management enables organizations to align security controls with their defined risk appetite rather than relying solely on external compliance requirements. This alignment allows leadership to make conscious, informed decisions about where to accept risk and where mitigation is necessary.

Risk-based approaches also encourage continuous reassessment rather than periodic compliance checks. As business environments change, new technologies are introduced, and threat actors adapt, organizational risk profiles evolve. Cremer (2022) notes that static security assessments often fail to capture emerging risks, whereas ongoing risk evaluation supports more responsive and adaptive security strategies. Continuous risk assessment ensures that cybersecurity management remains relevant and aligned with organizational priorities.

From a change management perspective, adopting risk-based decision-making represents a shift in how organizations measure cybersecurity success. Success is no longer defined solely by audit results or regulatory compliance, but by an organization’s ability to anticipate threats, respond effectively to incidents, and minimize business impact. This shift requires leadership support, clear communication, and a willingness to move beyond traditional compliance metrics. When organizations embrace risk-based prioritization, cybersecurity becomes an integral part of strategic planning rather than a reactive or isolated function.

While risk-based cybersecurity frameworks provide structure, their real value lies in how they support organizational decision-making. Risk assessment allows organizations to move beyond generalized security controls and focus attention on threats that pose the greatest potential harm. Rather than asking whether a control exists, risk assessment asks whether a threat could disrupt critical operations, compromise sensitive information, or create long-term business impact.

Risk assessment also enables prioritization in environments where resources are limited. Most organizations cannot address every vulnerability at once, which makes decision-making unavoidable. By evaluating risks based on likelihood and impact, leaders can determine which security issues require immediate mitigation and which risks can be temporarily accepted.

Landoll (2021) notes that structured risk assessments improve accountability by making these decisions explicit rather than implicit.

Another advantage of risk assessment is its ability to adapt to change. Compliance audits are typically performed at fixed intervals, while risk profiles evolve continuously as technologies, threats, and business processes change. Cremer (2022) emphasizes that static assessments often fail to capture emerging risks, particularly those associated with new attack techniques. Ongoing risk assessment allows organizations to adjust priorities as conditions change, reducing reliance on outdated assumptions.

From a management perspective, risk assessment strengthens communication between technical teams and leadership. When cybersecurity risks are framed in terms of business impact rather than technical details, executives are better positioned to understand trade-offs and support informed decision-making. This alignment reinforces cybersecurity as a business concern rather than a purely technical or compliance-driven function.

Integrating Cybersecurity with Enterprise Risk Management

Cybersecurity risks do not exist on their own and are part of broader organizational risks that include financial, operational, legal, and reputational risks. Integrating cybersecurity into enterprise risk management allows organizations to evaluate cyber threats alongside other business risks and make informed strategic decisions.

Stine et al. (2020) emphasize that treating cybersecurity as an enterprise risk enhances governance and accountability. When cyber risks are elevated to the executive and board level, organizations are better positioned to align security investments with business objectives. This integration also supports more effective communication between technical teams and leadership, reducing the gap between security operations and strategic decision-making.

Haque et al. (2025) argue that digital transformation has increased the need for integrated risk management approaches. As organizations adopt cloud computing, remote work, and interconnected systems, cybersecurity risks become more complex and interconnected. A risk-based ERM approach enables organizations to assess how cyber incidents could disrupt operations, impact customers, or undermine strategic goals.

Landoll (2021) further supports the role of structured risk assessments in improving security outcomes. By systematically evaluating threats and vulnerabilities, organizations can move beyond compliance-driven audits and develop more resilient security strategies. Risk assessments provide actionable insights that inform both technical controls and organizational policies.

Compliance and Risk Management in Practice

While compliance and risk management are often viewed as opposing approaches, they are not mutually exclusive. Compliance frameworks can provide a foundation upon which risk-based strategies are built. Kulshrestha et al. (2024) note that regulatory requirements can serve as baseline controls, while risk assessments help organizations tailor security measures to specific environments and technologies.

In practice, organizations that balance compliance with risk management are better positioned to address both regulatory expectations and real-world threats. Trinity and Sharma (2023) highlight the importance of balancing privacy, regulation, and security, particularly in environments where legal obligations and operational risks interact. A risk-based approach allows organizations to make informed trade-offs and prioritize protections that align with both regulatory and business needs.

The challenge lies in shifting organizational culture away from compliance-only thinking. Yusif and Hafeez-Baig (2023) suggest that effective cybersecurity governance requires leadership commitment and ongoing education. When employees understand the purpose behind security controls and how they relate to risk, compliance becomes more meaningful and effective.

Implications for Cybersecurity Change Management

Adopting a risk-based approach to cybersecurity requires organizational change. Processes, policies, and decision-making structures must evolve to support continuous risk assessment and adaptation. This shift aligns closely with the goals of cybersecurity change management, which emphasizes flexibility, learning, and strategic alignment.

Risk-based cybersecurity management encourages organizations to view security as an ongoing process rather than a one-time compliance effort. By continuously evaluating threats and adjusting controls, organizations can respond more effectively to change. This approach also supports better collaboration between technical teams, management, and stakeholders, fostering a shared understanding of risk.

From a managerial perspective, risk-based security supports more informed decision-making. Leaders can evaluate cybersecurity investments based on potential impact rather than regulatory pressure alone. This alignment improves resource allocation and strengthens organizational resilience in the face of uncertainty.

Conclusion

Compliance frameworks play a critical role in establishing baseline cybersecurity practices and meeting regulatory expectations. However, compliance alone is not sufficient to address the complexity and pace of modern cyber threats. As organizations continue to rely on digital systems, the limitations of compliance-driven security become increasingly evident.

A risk-based approach to cybersecurity management offers a more effective and adaptable strategy. By focusing on threat likelihood, asset value, and potential impact, organizations can prioritize security efforts that align with business objectives and evolving risks. Integrating cybersecurity into enterprise risk management further enhances governance, accountability, and strategic decision-making.

Ultimately, moving beyond compliance requires a change in how organizations think about cybersecurity must be viewed not as a checklist requirement but as a dynamic risk management process. Organizations that embrace this approach are better equipped to navigate change, protect critical assets, and sustain trust in an increasingly digital world.

References

AL-Dosari, K., & Fetais, N. (2023). Risk-management framework and information-security systems for small and medium enterprises (SMEs): A meta-analysis approach. *Electronics, 12*(17), 3629. https://doi.org/10.3390/electronics12173629

Aljumaiah, O., Jiang, W., Reddy Addula, S., & Almaiah, M. A. (2025). Analyzing cybersecurity risks and threats in IT infrastructure based on the NIST framework. *Journal of Cyber Security and Risk Auditing, 2025*(2), 12–26. https://doi.org/10.63180/jcsra.thestap.2025.2.2

Cremer, F. (2022). Cyber risk and cybersecurity: A systematic review of data availability and risk studies. *Journal of Cybersecurity Research*. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8853293/

Haque, G. M. M., Akula, D. K., Mohammed, Y. S., Syed, A., & Arafat, Y. (2025). Cybersecurity risk management in the age of digital transformation: A systematic literature review. *American Journal of Engineering and Technology, 7*(8), 126–150. https://emergingsociety.org/index.php/eflajet/article/view/255

Joshi, C., & Singh, U. K. (2017). Information security risks management framework: A step towards mitigating security risks in university networks. *Journal of Information Security and Applications, 35*, 128–137. https://doi.org/10.1016/j.jisa.2017.06.006

Kulshrestha, S., Acharya, N., Pal, R., & Vijayvargiya, L. (2024). IoT and cybersecurity regulations: Compliance and risk management strategies. In *Proceedings of the 2024*

International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES) (pp. 1–5). https://doi.org/10.1109/ICSES63760.2024.10910714

Landoll, D. (2021). *The security risk assessment handbook: A complete guide for performing security risk assessments* (3rd ed.). CRC Press. https://doi.org/10.1201/9781003090441

Security compliance and its implication for cybersecurity. (2024). *World Journal of Advanced Research and Reviews, 24*(1), 2105–2121. https://wjarr.com/sites/default/files/WJARR-2024-3170.pdf

Stine, K., Quinn, S., Witte, G., & Gardner, R. (2020). *Integrating cybersecurity and enterprise risk management (ERM)* (NIST Interagency Report 8286). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8286

Sulaiman, N. S., Fauzi, M. A., Wider, W., Rajadurai, J., Hussain, S., & Harun, S. A. (2022). Cyber–information security compliance and violation behavior in organizations: A systematic review. *Social Sciences, 11*(9), 386. https://doi.org/10.3390/socsci11090386

Taherdoost, H. (2022). Understanding cybersecurity frameworks and information security standards: A narrative review. *Electronics, 11*(14), 2181. https://www.mdpi.com/2079-9292/11/14/2181

Trinity, G. H., & Sharma, N. (2023). Cybersecurity regulations and compliance: Balancing privacy and protection in the digital age. In *Proceedings of the 2023 Seventh*

International Conference on Image Information Processing (ICIIP) (pp. 794–799). https://doi.org/10.1109/ICIIP61524.2023.10537636

Yusif, S., & Hafeez-Baig, A. (2023). Cybersecurity policy compliance in higher education: A theoretical framework. *Journal of Applied Security Research*, *18*(2), 267–288. https://doi.org/10.1080/19361610.2021.1989271