Novatio: Journal of Management Technology and Innovation
E-ISSN : 3030-8674
Volume. 2, Issue 3, July 2024
Page No: 189-204

Integrating Governance, Technical Controls, and Agile Practices: A Multi Layered Risk Management Framework for High Technology Projects

Heri Hermansyah[1], Ricky Muhamad Zakaria[2]
[1]Badan Kepegawaian dan Diklat Kabupaten Garut, Indonesia
[2]Universitas Garut, Indonesia
Correspondent : hermansyah80@garutkab.go.id[1]

Received : June 2, 2024
Accepted : July 18, 2024
Published : July 31, 2024

Citation: Hermansyah, H., Zakaria, R, M.. (2024). Integrating Governance, Technical Controls, and Agile Practices: A Multi Layered Risk Management Framework for High Technology Projects. Novatio: Journal of Management Technology and Innovation, 2(3), 189-204.

ABSTRACT: High technology project environments present a complex landscape of interdependent risks spanning governance, technical, and operational domains. This study examines the integration of governance structures, domain specific technical controls, and agile risk management practices to address these multifaceted challenges. The research highlights the strategic synergy between frameworks such as ISO 31000, ISO/IEC 27005, NIST SP 800 53, and the NIST AI RMF, combined with agile techniques like SAFe ROAM, to create a comprehensive, layered risk management architecture. This approach enables precise risk identification, robust mitigation planning, and responsive adaptation to rapidly evolving technological and market conditions. The methodology involved analyzing best practices in cross framework integration, risk mapping, and agile tracking methods, supported by case studies and empirical literature. Key findings show that multi-layered frameworks improve adaptability, strengthen decision making, and enhance transparency. They also create a shared risk language across technical, managerial, and executive levels, which improves communication and coordination. Results reveal that challenges persist, including coordination complexity, cultural resistance, and potential duplication when frameworks are not harmonized. Addressing these issues requires deliberate integration planning, stakeholder engagement, and change management strategies. In addition, adopting AI and automation improves real-time risk detection, dynamic control mapping, and continuous monitoring. These capabilities help organizations maintain compliance and resilience in rapidly changing regulatory environments. In conclusion, multi layered risk management frameworks represent a strategic imperative for organizations operating in high tech sectors. By combining governance oversight, technical precision, and agile adaptability, these frameworks deliver resilience, foresight, and agility essential for sustainable growth and long term competitive advantage.

Keywords: Risk Management, High Technology Projects, ISO 31000, NIST SP 800 53, Agile Risk Management.

INTRODUCTION

High technology projects present an exceptionally complex and dynamic risk landscape due to the interplay of advanced, interdependent systems, diverse stakeholder groups, and rapidly evolving technological and market conditions. The management of multi domain risks in such projects is complicated by the convergence of cybersecurity, compliance, operational, and strategic concerns, each of which can influence and amplify the others. As noted by Folorunso et al. (2024), the multidimensional nature of risks in high tech environments creates interdependencies that, if not effectively managed, can lead to cascading failures. A breach in information security, for example, may not only result in data loss but also trigger compliance violations, operational disruption, and severe reputational damage (Babalola et al., 2024). Such interconnectedness necessitates a holistic and coordinated approach that explicitly addresses cross domain dependencies.

The challenges in managing these risks are exacerbated by the pace of technological advancement. As new capabilities such as artificial intelligence (AI), machine learning, and advanced cloud computing emerge, they introduce both opportunities and vulnerabilities. Radanliev et al. (2023) observe that derivative risks frequently arise as unintended consequences of these technologies. AI driven solutions, while potentially enhancing security, also introduce risks including algorithmic bias, adversarial manipulation, and model drift (Akhtar & Rawol, 2024). Similarly, the migration to cloud based infrastructures offers scalability and resilience but introduces risks related to vendor lock in, data governance complexities, and compliance with diverse jurisdictional requirements. Traditional risk management approaches often fail to account for the sophistication and velocity of emerging threats, with many organizations struggling to keep pace with developments in the threat landscape (Camacho, 2024). The result is often gaps in risk management frameworks, leading to inadequate preparation for novel risk scenarios and diminished organizational resilience (Patil et al., 2024).

Enterprise Risk Management (ERM) principles, as defined by the ISO 31000 standard, provide a governance focused foundation for addressing organizational risks across all contexts. ISO 31000 outlines principles that emphasize integration of risk management into corporate governance structures, the creation of a holistic framework, and the promotion of a risk aware culture through continuous communication and stakeholder engagement (Barrett et al., 2021). However, while ISO 31000 provides broad governance coverage, it lacks technical specificity. Existing studies often address governance or technical controls separately but rarely integrate them into a single multi-layered model. This gap highlights the need for a comprehensive framework that connects governance, domain-specific controls, and agile operational practices.Its lifecycle approach comprises risk assessment, risk treatment, monitoring, and review, all of which must be adapted to the organization's evolving internal and external environment (Familoni, 2024). This structured approach is particularly vital in high tech projects, where both technological and regulatory landscapes change rapidly, requiring adaptive and agile risk management mechanisms (Okoye et al., 2024).

Empirical studies provide strong evidence in support of integrating multiple frameworks into a cohesive risk management approach. Kure et al. (2018) found that cross functional integration enhances risk visibility, supports more effective decision making, and strengthens organizational resilience. Organizations employing such integration are better equipped to anticipate potential threats and respond effectively to incidents when they occur (Pasupuleti et al., 2025). Integrated frameworks also facilitate compliance with regulatory requirements by aligning strategies across different levels of governance (Folorunso et al., 2024). Importantly, the harmonization of governance focused frameworks like ISO 31000 with technical control standards such as NIST SP 800 53 enables process standardization while maintaining the flexibility to address specific organizational needs (Barrett et al., 2021). This interoperability not only streamlines compliance activities but also fosters knowledge sharing and best practices across sectors, improving resilience in the face of evolving threats (Kloukiniotis et al., 2022).

Despite these advantages, governance gaps remain a significant challenge in high tech project environments. Inadequate governance structures can lead to misaligned objectives, unclear roles and responsibilities, and weak oversight mechanisms. Jerbi (2023) highlights that such deficiencies often result in the failure to identify or adequately manage critical risks, leading to cost overruns, project delays, or compromised outcomes. Governance mechanisms that fail to incorporate emerging risks particularly those associated with AI and multi cloud infrastructures are at heightened risk of breakdown (Kaur et al., 2024). Technological change frequently outpaces both internal governance structures and external regulatory frameworks, creating compliance gaps that can jeopardize project goals (Katrakazas & Papastergiou, 2024).

The technological trends shaping contemporary risk management practices are significant. In AI, recent advances have enabled organizations to leverage predictive analytics for proactive risk assessment, identifying anomalies and potential threats in real time (Mavani, 2025). These capabilities shift risk management from reactive to proactive, enabling faster and more informed interventions (Al-Quayed et al., 2024). In the realm of cloud computing, organizations are increasingly adopting multi cloud strategies to enhance system resilience. While such strategies reduce dependence on a single provider, they introduce complexities in security architecture, data governance, and compliance monitoring (Kalva et al., 2024). Cybersecurity remains central to this discourse; as threats become more sophisticated, the integration of advanced defensive measures such as zero trust architectures and AI driven intrusion detection is becoming indispensable (Owolabi et al., 2024).

The literature on cross framework interoperability reinforces the case for integrated risk management in high tech contexts. Studies show that harmonizing governance standards like ISO 31000 with technical standards such as NIST SP 800 53 and COBIT results in greater organizational agility, reduced redundancy, and improved capacity to respond to emerging risks (Wang et al., 2025). These benefits are amplified when integration is accompanied by artefacts that map risk scenarios to relevant controls, facilitating traceability and accountability across organizational layers.

However, despite recognition of these benefits, there remains a notable gap in the literature. Few models provide a structured method for integrating governance, domain specific, and operational frameworks into a single architecture designed for high tech projects. Existing integrations tend to focus narrowly on compliance alignment or technical interoperability, without adequately addressing how risks should flow between strategic, domain specific, and execution layers. Addressing this gap requires a comprehensive framework capable of linking high level governance with specialized technical controls and agile operational processes.

This study aims to develop and evaluate a three layer risk management model tailored to the needs of high tech project environments. The first layer, governance and process, draws on ISO 31000 to establish enterprise level policy, risk appetite, and review cycles. The second layer focuses on domain specific controls, incorporating frameworks such as ISO/IEC 27005, NIST SP 800 53, NIST AI RMF, EU AI Act, and NASA NPR 8000.4C to provide technical and regulatory depth. The third layer addresses operational execution through agile methods such as SAFe ROAM, enabling real time risk tracking and mitigation at the program and sprint levels. The novelty of this model lies in its explicit mapping of risks across these three layers, supported by practical artefacts including a unified risk register, control matrices, AI risk profiles, and burndown charts. By uniting governance, technical depth, and operational agility, the proposed layered stack aims to close the persistent gap between strategic oversight and day to day execution in high tech risk management.

METHOD

The methodology began with identifying the criteria for selecting risk management frameworks that are suitable for high tech project environments. Previous studies emphasize that the effectiveness of framework selection depends on its alignment with the specific operational needs and strategic objectives of the organization (Blair et al., 2024). This alignment ensures that risk management practices integrate seamlessly with existing organizational structures, governance processes, and corporate culture. In high tech contexts, where technologies, market demands, and threat landscapes shift rapidly, adaptability becomes a primary requirement. Frameworks must be capable of accommodating evolving enterprise architectures and dynamic risk profiles, providing flexibility for continuous improvement over time (Hoang et al., 2025).

Another crucial criterion is comprehensiveness. A suitable framework must allow organizations to identify, assess, and address a wide spectrum of risks from natural disasters to complex cyber threats within a unified approach (Cheimonidis & Rantos, 2023). This requires the incorporation of robust risk assessment methodologies that facilitate the quantification and prioritization of risks, allowing decision makers to apply data driven strategies for resilience (Du et al., 2020). Additionally, literature indicates that frameworks incorporating stakeholder engagement mechanisms foster a culture of collaboration and accountability in risk management. Such engagement is particularly valuable in high tech projects, where innovation and execution depend heavily on cross functional teams(Lai & Ishizaka, 2020).

A core methodological element in this study involved mapping identified risk scenarios to corresponding technical controls, using NIST SP 800 53 as the primary reference standard. The NIST SP 800 53 framework provides a comprehensive catalogue of management, operational, and technical security controls. The mapping process follows a structured sequence that begins with asset identification, threat recognition, and vulnerability analysis (Kure et al., 2018). Once risks are categorized based on severity and likelihood, high priority risks are matched to controls selected according to the organization’s risk tolerance, regulatory obligations, and overarching risk philosophy (Ganin et al., 2017).

This process adopts a tiered approach, enabling targeted allocation of resources to the most critical risks. The methodology emphasizes continuous monitoring and revision of the mapping as the organization's environment and threat landscape evolve. This requires ongoing collaboration between IT security teams and enterprise risk managers to ensure controls remain relevant and effective against emerging threats (Ganin et al., 2017; Mansour, 2022). To enhance the mapping process, organizations often utilize specialized tools for risk analysis and control selection, which provide transparency and support evidence based decision making (Lee & Wang, 2023).

Given the prevalence of agile methodologies in high tech project delivery, the integration of agile risk tracking into enterprise governance structures formed another methodological priority. Techniques such as Agile Risk Management (ARM) and Continuous Risk Assessment (CRA) offer iterative evaluation cycles that enable organizations to adapt quickly to new risks and information (Islam et al., 2024; Tiwari, 2024). Incorporating these methods into governance frameworks involves creating hybrid models that combine the flexibility of agile practices with the stability and oversight provided by traditional governance processes(Islam et al., 2024; Krishankumar et al., 2022).

Effective integration requires establishing formal channels of communication between agile delivery teams and governance bodies, ensuring that operational risk insights are visible to decision makers at the strategic level (Tiwari, 2024). This can be facilitated through shared artefacts such as unified risk registers, risk burndown charts, and escalation workflows that link operational incidents to governance oversight. Real time risk tracking tools are also instrumental in enabling rapid decision making and maintaining compliance with both regulatory and internal standards. By combining agile responsiveness with structured governance, the organization enhances its resilience and aligns operational agility with long term strategic objectives.

The methodological framework for this research integrates three critical components. First, framework selection was guided by alignment, adaptability, comprehensiveness, and stakeholder engagement. Second, risk-to-control mapping followed a systematic, tiered approach grounded in NIST SP 800-53, ensuring traceability from identification to treatment. Third, agile risk tracking was embedded into governance structures, establishing a continuous feedback loop between operational execution and strategic oversight.

By combining these elements, the resulting three layer risk management stack draws on ISO 31000 for governance, ISO/IEC 27005 and NIST SP 800 53 for domain specific control, and SAFe ROAM or similar agile methods for operational execution. This integration ensures comprehensive coverage of multi domain risks, supports proactive adaptation to emerging threats, and aligns risk management with both regulatory requirements and strategic objectives. The methodology also anticipates the inclusion of new standards such as the EU AI Act and NASA NPR 8000.4C as technological and regulatory contexts evolve.

Overall, these methodological steps ensured that the framework was not only theoretically grounded but also practically operationalized for high-tech project environments. This provides a smoother transition from theoretical background to framework design.

RESULT AND DISCUSSION

Governance & Process

The governance and process layer is anchored in ISO 31000, which provides comprehensive guidance for policy setting, risk appetite definition, and review cycles. The standard emphasizes integrating risk management into the organizational governance framework, ensuring policy alignment with strategic objectives and operational goals (Bao et al., 2024; Uwadi et al., 2022). Defining a clear risk appetite helps organizations determine the types and levels of risk they are prepared to accept, thereby embedding risk considerations into decision making processes at all levels. Regular review cycles serve as a continuous improvement mechanism, allowing risk management policies to adapt to changing internal and external risk environments.

Case studies highlight the effectiveness of ISO 31000 in high tech industries. One major technology corporation applied ISO 31000 to establish a robust governance driven risk system, reducing operational risks and increasing stakeholder confidence (Lewis, 2022). Similarly, a high tech startup used ISO 31000 to streamline its risk assessments, improving project agility and outcomes (Batista et al., 2022). These examples show how the framework fosters a culture of proactive governance and enhances the strategic alignment of risk management.

Enterprise risk registers are critical tools in this layer, especially when structured to track cross domain risks. Well-designed registers capture severity, likelihood, ownership, and mitigation strategies, offering a holistic view across functions such as cybersecurity, compliance, and delivery (Binamungu & Mahundi, 2022). Governance artifacts such as risk dashboards and committee reports further enhance executive oversight, ensuring transparency, accountability, and strategic alignment (Mamais et al., 2022).

Domain Specific Controls

This layer operationalizes risk management for specific domains, beginning with ISO/IEC 27005 for structured information security risk assessments. The standard outlines systematic processes for identification, assessment, treatment, and continuous monitoring, enabling tailored controls to address context specific vulnerabilities. Outputs from ISO/IEC 27005 can be system(Wiedemann, 2018) atically mapped to NIST SP 800 53 controls using risk matrices, linking identified vulnerabilities to specific security controls based on severity and regulatory requirements (Verma & Tyagi, 2025).

The NIST AI RMF addresses AI specific risks such as bias, drift, and misuse, recommending continuous monitoring of AI system performance and fairness throughout the lifecycle (Alamri et al., 2024). This is complemented by the EU AI Act, which mandates classification and compliance for high risk AI systems, requiring risk assessments, transparency, and monitoring for domains such as biometric identification and critical infrastructure (Akerele et al., 2024).

Table 1. Framework–Function Mapping

Framework	Core Function	Layer	Outputs/Artefacts	Dependencies
ISO 31000	Governance & lifecycle	1	Risk Policy, Appetite Statement, ERM Register	None
ISO/IEC 27005	Infosec risk assessment & treatment	2	Risk Scenarios, Treatment Plan	ISO 31000
NIST SP 800 53	Technical & privacy controls	2	Control Matrix, SSP, PoA&M	ISO/IEC 27005
NIST AI RMF	AI specific risk governance	2	AI Risk Profile, Monitoring Plan	ISO 31000
EU AI Act	AI risk classification & compliance	2	Risk Class, Conformity Docs	NIST AI RMF
SAFe ROAM	Agile risk tracking	3	ROAM Log, Burndown Chart	ISO 31000
NASA NPR 8000.4C	Critical system hazard management	2/3	Hazard Log, Tech Readiness Reviews	ISO 31000

Operational Execution

Operational execution integrates SAFe ROAM into program level risk tracking, categorizing risks as Resolved, Owned, Accepted, or Mitigated (Salameh & Bass, 2021). This iterative approach embeds risk management into agile planning, enabling teams to adapt to emerging challenges (Karampa & Paraskeva, 2024). Maintaining risk burndown charts is essential for tracking progress and providing real time visibility to stakeholders (Simard & Lapalme, 2019).

Escalation workflows between agile teams and governance bodies ensure that critical risks receive strategic attention, though poorly defined workflows can cause bottlenecks (Wijaya et al., 2024). NASA's NPR 8000.4C complements these practices for mission critical systems, enforcing standardized risk analysis and mitigation tracking (Gent et al., 2017).

Table 2 . Risk Scenario → Control Mapping

Risk Scenario	ISO/IEC 27005 Ref.	NIST SP 800 53 Control	AI RMF Function	ROAM Status
AI model bias	8.2.2	PT 2 Privacy Notice	MEASURE	Mitigated
Cloud vendor lock in	8.2.3	CP 10 System Recovery	MANAGE	Owned
Supply chain data leak	8.2.1	SA 12 Supply Chain Protection	MANAGE	Resolved
HW–SW interface failure	8.2.4	SI 7 Interface Protection	MANAGE	Accepted
AI hallucination	8.2.2	SI 10 Input Validation	MEASURE	Mitigated

Cross Layer Mapping and Metrics

Traceability matrices enable a structured relationship between risks, controls, and compliance requirements, reducing duplication and ensuring clear oversight (Shaik, 2024). Harmonizing artifacts across layers requires unified definitions and periodic documentation reviews (Paul et al., 2025).

Key metrics for cross layer performance include risk exposure levels, incident frequency, and mitigation resource allocation (Vududala, 2020). These metrics not only assess risk reduction effectiveness but also strengthen audit readiness and regulatory compliance (Matthies et al., 2016).

Table 3. Risk Burndown Tracking (8 Weeks)

Week	Total Risks	Resolved	Mitigated	Accepted	Owned
1	25	0	3	2	20
2	25	2	5	2	16
4	20	6	8	3	6
8	12	12	8	2	0

Benefits of Integrating Governance, Technical Controls, and Agile Risk Management

Integrating governance frameworks, technical controls, and agile risk management methods yields a wide array of strategic and operational benefits, particularly in high tech industries characterized by rapid innovation cycles and complex stakeholder environments. One of the most prominent advantages is enhanced adaptability. By combining the disciplined structure of governance principles with the flexibility inherent in agile methodologies, organizations can react swiftly to changes in technology, market demands, and threat landscapes, while incorporating stakeholder feedback in near real time (Pinto, 2023). Agile practices enable continuous client engagement, iterative refinement of deliverables, and realignment of priorities, ensuring that evolving requirements are met without compromising quality or compliance.

Transparency and accountability are equally significant outcomes. Governance frameworks provide structured mechanisms for monitoring risks, evaluating mitigation effectiveness, and ensuring alignment with strategic objectives (Vieira et al., 2020). This visibility fosters a culture of responsibility across all levels, bridging the gap between high-level strategies and daily operations, and reinforcing alignment between organizational goals and practical execution. Prior studies also highlight similar outcomes, showing that governance-aligned risk practices improve compliance and stakeholder trust

The integration also elevates decision making processes. Combining agile risk management approaches with formal governance mechanisms produces comprehensive risk profiles that inform both strategic choices and operational adjustments (Surenthran et al., 2024). Early identification of emerging risks enables proactive deployment of targeted controls, reducing the likelihood of costly delays or disruptions (Thom-Manuel, 2022). Evidence suggests that explicit risk management within agile environments enhances delivery timelines, strengthens problem solving capacity, and increases stakeholder satisfaction (Babayev & QULUZADA, 2025). Additionally, this integration creates a shared language for risk, facilitating communication between technical teams, project managers, and executive leadership.

Challenges in Implementing Multi Layered Risk Frameworks

Despite the substantial benefits, implementing a multi layered risk framework is not without challenges. Coordination across different governance layers can be complex, as each may operate under different priorities, reporting systems, and compliance expectations. Such misalignment can lead to communication breakdowns and fragmented insights, undermining the goal of holistic risk management (Rahman, 2024).

Resistance to change is another recurring barrier. Teams accustomed to established workflows may resist integrating new processes, especially when they require the harmonization of diverse methodologies such as Agile, Lean, and traditional risk management (Ononiwu, 2025). Without robust change management strategies, these differences can create friction, reduce collaboration, and slow down adoption.

There is also the risk of duplication when frameworks overlap without clear coordination. Redundant processes can waste resources, generate confusion about responsibilities, and complicate decision making. Therefore, integration must be carefully planned, documented, and communicated to ensure clarity and efficiency.

Role of AI and Automation in Enhancing Integrated Risk Frameworks

AI and automation present transformative opportunities for strengthening integrated frameworks. Automation tools standardize and expedite routine tasks such as risk identification, control mapping, and progress tracking reducing human error and freeing resources for strategic oversight (Tak & Chahal, 2024). These functions connect directly to governance goals by ensuring consistency, while also supporting agile teams through real-time updates. Thus, automation bridges the structural focus of governance with the adaptability of agile practices.

AI driven analytics can process vast datasets, including operational metrics and threat intelligence, to detect anomalies, identify vulnerabilities, and forecast emerging risks with greater accuracy than manual analysis (Handaragal, 2025). Machine learning models further contribute by dynamically updating risk profiles as new data emerges, ensuring that mitigation strategies remain relevant and responsive (Tak & Chahal, 2024). In fast moving high tech environments, these capabilities are critical for sustaining resilience and maintaining competitive advantage.

4.4 Implications for Regulatory Alignment in High Tech Sectors

Multi layered risk frameworks also have profound implications for regulatory compliance in high tech sectors, where evolving regulations must keep pace with technological advancements. Integrated approaches allow organizations to embed compliance into daily workflows, ensuring that legal and regulatory requirements are met continuously rather than sporadically (García et al., 2024).

By enabling proactive compliance monitoring, integrated frameworks help organizations adapt quickly to legislative changes without disrupting operations. This is particularly valuable in sectors where innovation cycles are short, and compliance breaches can result in significant financial and reputational damage(Gobile & Awoyemi, 2025). In effect, such frameworks offer the agility to pivot when regulations change while preserving operational efficiency and innovation capacity.

CONCLUSION

This study demonstrates that integrating governance structures, domain-specific technical controls, and agile risk management practices provides a distinctive and comprehensive framework for managing risks in high-technology project environments. The novelty lies in the explicit mapping of risks across three interconnected layers governance, technical, and operational supported by practical artefacts such as unified risk registers, control matrices, AI risk profiles, and burndown charts. Unlike prior approaches that address governance or technical issues in isolation, this layered model offers a unified and adaptable structure. For practitioners, the framework delivers actionable guidance to improve decision-making, strengthen resilience, and maintain regulatory alignment, while for policymakers it highlights pathways to embed compliance and innovation into sectoral governance systems.

Despite its contributions, the research also faces limitations, particularly the reliance on case-based evidence rather than large-scale empirical validation. Future studies should incorporate broader datasets and longitudinal analyses to test the scalability and long-term impact of integrated frameworks across diverse sectors. Nevertheless, the findings point to a forward-looking trajectory in which AI and automation further enhance risk management through real-time detection, adaptive control mapping, and continuous monitoring. Ultimately, adopting multi-layered frameworks is not only a best practice but a strategic imperative, offering organizations the resilience, foresight, and agility required to thrive in rapidly evolving technological and regulatory landscapes.

REFERENCE

Akerele, J. I., Uzoka, A., Ojukwu, P. U., & Olamijuwon, O. J. (2024). Increasing Software Deployment Speed in Agile Environments Through Automated Configuration Management. *International Journal of Engineering Research Updates*, *7*(2), 028–035. https://doi.org/10.53430/ijeru.2024.7.2.0047

Akhtar, Z. B., & Rawol, A. T. (2024). Harnessing Artificial Intelligence (AI) for Cybersecurity: Challenges, Opportunities, Risks, Future Directions. *Comput. Artif. Intell.*, *2*(2), 1485. https://doi.org/10.59400/cai.v2i2.1485

Alamri, A., Harfash, S., & Alsaleem, N. (2024). Comparative Analysis of Traditional, Agile, and Flexible Management Approaches (Exploring Differences, Compatibility, and Impacts on

Organizational Performance). *Academic Journal of Research and Scientific Publishing*, *6*(67), 143–155. https://doi.org/10.52132/ajrsp.e.2024.67.6

Al-Quayed, F., Ahmad, Z., & Humayun, M. (2024). A Situation Based Predictive Approach for Cybersecurity Intrusion Detection and Prevention Using Machine Learning and Deep Learning Algorithms in Wireless Sensor Networks of Industry 4.0. *Ieee Access*, *12*, 34800–34819. https://doi.org/10.1109/access.2024.3372187

Babalola, D. O., Adedoyin, A., Ogundipe, F., Folorunso, A., & Nwatu, C. E. (2024). Policy Framework for Cloud Computing: AI, Governance, Compliance and Management. *Global Journal of Engineering and Technology Advances*, *21*(2), 114–126. https://doi.org/10.30574/gjeta.2024.21.2.0212

Babayev, I., & QULUZADA, S. (2025). Integration of Modern Methodologies With Pmo in the Management of Investment Projects. *Economics of the Transport Complex*, *45*, 171. https://doi.org/10.30977/etk.2225-2304.2025.45.171

Bao, Y., Cheng, X., Su, L., & Zarifis, A. (2024). Achieving Employees' Agile Response in E-Governance: Exploring the Synergy of Technology and Group Collaboration. *Group Decision and Negotiation*, *34*(2), 209–234. https://doi.org/10.1007/s10726-024-09911-y

Barrett, M., Marron, J., Pillitteri, V., Boyens, J. M., Quinn, S., Witte, G., & Feldman, L. (2021). *Approaches for Federal Agencies to Use the Cybersecurity Framework*. https://doi.org/10.6028/nist.ir.8170-upd

Batista, F., Pereira, L., Costa, R. L. D., & António, N. (2022). Agile Project and Portfolio Management: A Systematic Literature Review. *International Journal of Process Management and Benchmarking*, *12*(4), 471. https://doi.org/10.1504/ijpmb.2022.123742

Binamungu, L. P., & Mahundi, M. (2022). Investigating the Support for Agility in Developing Government Software Systems: A Case of Three East African Countries. *Tanzania Journal of Engineering and Technology*, *41*(3), 1–13. https://doi.org/10.52339/tjet.v41i3.839

Blair, G., Woodcock, H., Pagano, R., & Endlar, L. (2024). Constructing a Risk Management Framework to Protect the Organization. *J.UTEC.Eng.Manag*, *2*(01), 113–124. https://doi.org/10.36344/utecem.2024.v02i01.010

Camacho, N. (2024). The Role of AI in Cybersecurity: Addressing Threats in the Digital Age. *Jaigs*, *3*(1), 143–154. https://doi.org/10.60087/jaigs.v3i1.75

Cheimonidis, P., & Rantos, K. (2023). Dynamic Risk Assessment in Cybersecurity: A Systematic Literature Review. *Future Internet*, *15*(10), 324. https://doi.org/10.3390/fi15100324

Du, J., Peng, S., & Jisheng, P. (2020). Research on Technology Innovation Risk Evaluation of High-Tech Enterprises Based on Fuzzy Evaluation. *Journal of Intelligent & Fuzzy Systems*, *38*(6), 6805–6814. https://doi.org/10.3233/jifs-179758

Familoni, B. T. (2024). Cybersecurity Challenges in the Age of Ai: Theoretical Approaches and Practical Solutions. *Computer Science & It Research Journal*, *5*(3), 703–724. https://doi.org/10.51594/csitrj.v5i3.930

Folorunso, A., Adewumi, T., Adewa, A., Okonkwo, R., & Olawumi, T. N. (2024). Impact of AI on Cybersecurity and Security Compliance. *Global Journal of Engineering and Technology Advances*, *21*(1), 167–184. https://doi.org/10.30574/gjeta.2024.21.1.0193

Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., & Linkov, I. (2017). Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management. *Risk Analysis*, *40*(1), 183–199. https://doi.org/10.1111/risa.12891

García, F., Hauck, J. C. R., & Borgatto, A. F. (2024). *How Do Agile Organizations Manage Risks: An Analysis of the State of Practice in Brazil*. 80–91. https://doi.org/10.5753/sbes.2024.3292

Gent, I. v., Rocca, G. L., & Veldhuis, L. L. (2017). *Composing MDAO Symphonies: Graph-Based Generation and Manipulation of Large Multidisciplinary Systems*. https://doi.org/10.2514/6.2017-3663

Gobile, S., & Awoyemi, O. (2025). The Agile Legal Management Framework: Bridging Legal and Technology Gaps in Corporate Affairs. *International Journal of Scientific Research in Computer Science Engineering and Information Technology*, *11*(3), 761–773. https://doi.org/10.32628/cseit25113332

Handaragal, R. (2025). Agile for SCM/ERP Implementations: Challenges, Conflict Management, and Strategies for Success. *Journal of Information Systems Engineering & Management*, *10*(4), 1365–1378. https://doi.org/10.52783/jisem.v10i4.10657

Hoang, V. A., Thai, A., Le, P. U., Nguyen, T. H., & Dang, M. (2025). Corruption Control, High-Tech Acquisitions, and the Role of Power Distance. *Sage Open*, *15*(1). https://doi.org/10.1177/21582440251323664

Islam, S., Basheer, N., Silvestri, S., Papastergiou, S., & Ciampi, M. (2024). *Intelligent Dynamic Cybersecurity Risk Management Framework With Explainability and Interpretability of AI Models for Enhancing Security and Resilience of Digital Infrastructure*. https://doi.org/10.21203/rs.3.rs-4796809/v1

Jerbi, D. (2023). Beyond Firewalls: Navigating the Jungle of Emerging Cybersecurity Trends. *Journal of Current Trends in Computer Science Research*, *2*(2). https://doi.org/10.33140/jctcsr.02.02.14

Kalva, P., -, S. P., & -, S. C. (2024). Adaptive Security Paradigms: The Role of AI in Safeguarding Distributed Data Across Multi-Cloud Platforms. *International Journal for Multidisciplinary Research*, *6*(5). https://doi.org/10.36948/ijfmr.2024.v06i05.29551

Karampa, V., & Paraskeva, F. (2024). *Team Effectiveness of Higher Education Students Through Project-Based and Agile Education for Sustainable Development*. https://doi.org/10.54941/ahfe1004554

Katrakazas, P., & Papastergiou, S. (2024). A Stakeholder Needs Analysis in Cybersecurity: A Systemic Approach to Enhancing Digital Infrastructure Resilience. *Businesses*, *4*(2), 225–240. https://doi.org/10.3390/businesses4020015

Kaur, J., Hasan, S. H., Orthi, S. M., Miah, M. A., Goffer, M. A., Barikdar, C. R., & Hassan, J. (2024). Advanced Cyber Threats and Cybersecurity Innovation—Strategic Approaches and Emerging Solutions. *Journal of Computer Science and Technology Studies*, *5*(3), 112–121. https://doi.org/10.32996/jcsts.2023.5.3.9

Kloukiniotis, A., Papandreou, A. G., Lalos, A. S., Kapsalas, P., Nguyen, D.-V., & Μουστάκας, K. (2022). Countering Adversarial Attacks on Autonomous Vehicles Using Denoising Techniques: A Review. *Ieee Open Journal of Intelligent Transportation Systems*, *3*, 61–80. https://doi.org/10.1109/ojits.2022.3142612

Krishankumar, R., Mishra, A. R., Cavallaro, F., Zavadskas, E. K., Antuchevičienė, J., & Ravichandran, K. S. (2022). A New Approach to the Viable Ranking of Zero-Carbon Construction Materials With Generalized Fuzzy Information. *Sustainability*, *14*(13), 7691. https://doi.org/10.3390/su14137691

Kure, H. I., Islam, S., & Razzaque, M. A. (2018). An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System. *Applied Sciences*, *8*(6), 898. https://doi.org/10.3390/app8060898

Lai, Y., & Ishizaka, A. (2020). The Application of Multi-Criteria Decision Analysis Methods Into Talent Identification Process: A Social Psychological Perspective. *Journal of Business Research*, *109*, 637–647. https://doi.org/10.1016/j.jbusres.2019.08.027

Lee, K., & Wang, L.-Y. (2023). Chinese High-Tech Export Performance: Effects of Intellectual Capital Mediated by Dynamic and Risk Management Capabilities. *Sage Open*, *13*(1). https://doi.org/10.1177/21582440231153039

Lewis, A. (2022). Agile Project Management Facilitates Efficient and Collaborative Collection Development Work. *Evidence Based Library and Information Practice*, *17*(4), 170–172. https://doi.org/10.18438/eblip30221

Mamais, F., Jasdhaul, M., Gawlinski, A., Lawanson-Nichols, M., Kao, Y.-H., Branom, R., & Ansryan, L. Z. (2022). The Agile Clinical Nurse Specialist. *Clinical Nurse Specialist*, *36*(4), 190–195. https://doi.org/10.1097/nur.0000000000000682

Mansour, R. F. (2022). Artificial Intelligence Based Optimization With Deep Learning Model for Blockchain Enabled Intrusion Detection in CPS Environment. *Scientific Reports*, *12*(1). https://doi.org/10.1038/s41598-022-17043-z

Matthies, C., Kowark, T., Richly, K., Uflacker, M., & Plattner, H. (2016). *ScrumLint*. 40–43. https://doi.org/10.1145/2897586.2897602

Mavani, C. (2025). Enhancing Cybersecurity With AI and Machine Learning: Automated Threat Detection in DevOps and Cloud Environments. *Journal of Information Systems Engineering & Management*, *10*(37s), 875–886. https://doi.org/10.52783/jisem.v10i37s.6737

Okoye, C. C., Nwankwo, E. E., Usman, F. O., Mhlongo, N. Z., Odeyemi, O., & Ike, C. U. (2024). Accelerating SME Growth in the African Context: Harnessing FinTech, AI, and Cybersecurity for Economic Prosperity. *International Journal of Science and Research Archive*, *11*(1), 2477–2486. https://doi.org/10.30574/ijsra.2024.11.1.0231

Ononiwu, M. (2025). Investigating Agile Portfolio Management Techniques for Prioritizing Strategic Initiatives in Large-Scale Government IT Projects. *International Journal of Management & Entrepreneurship Research*, *7*(6), 464–483. https://doi.org/10.51594/ijmer.v7i6.1941

Owolabi, I. O., Mbabie, C. K., & Obiri, J. C. (2024). AI-Driven Cybersecurity in FinTech &Amp; Cloud: Combating Evolving Threats With Intelligent Defense Mechanisms. *Ijmrset*, *07*(12). https://doi.org/10.15680/ijmrset.2024.0712004

Pasupuleti, V. S. M., Gupta, R. K., & Rachamalla, D. (2025). Intelligent Cloud-Native Architectures for Secure, Scalable, and AI-Driven Digital Transformation in Retail and Insurance Domains. *PJCS*. https://doi.org/10.70389/pjcs.100009

Patil, D., Rane, N. L., & Rane, J. (2024). *Future Directions for ChatGPT and Generative Artificial Intelligence in Various Business Sectors*. https://doi.org/10.70593/978-81-981367-8-7_7

Paul, S., Bolesnikov, M., Stojanović, K., Silić, D., & Njegovan, M. (2025). *Strategy to Develop Project by Using Hybrid Approach*. *1*, 448–455. https://doi.org/10.24867/future-bme-2024-050

Pinto, H. W. (2023). Exploring the Implementation of Agile Project Management in the United States Construction Industry: Benefits, Challenges, and Success Factors. *Journal of Entrepreneurship & Project Management*, *7*(7), 11–23. https://doi.org/10.53819/81018102t4163

Radanliev, P., Roure, D. D., Maple, C., & Ani, U. (2023). *Super-Forecasting The 'technological Singularity' risks From Artificial Intelligence*. https://doi.org/10.21203/rs.3.rs-919939/v1

Rahman, A. (2024). It Project Management Frameworks: Evaluating Best Practices and Methodologies for Successful It Project Management. *Ajsteme*, *1*(01), 57–76. https://doi.org/10.69593/ajaimldsmis.v1i01.128

Salameh, A., & Bass, J. M. (2021). An Architecture Governance Approach for Agile Development by Tailoring the Spotify Model. *Ai & Society*, *37*(2), 761–780. https://doi.org/10.1007/s00146-021-01240-x

Shaik, S. (2024). Advancement of Incident Response Plans: Bridging Gaps in SDLC With Security Integration in Agile Development. *International Journal of Multidisciplinary Research and Growth Evaluation*, *5*(2), 1031–1034. https://doi.org/10.54660/.ijmrge.2024.5.2.1031-1034

Simard, M., & Lapalme, J. (2019). *Self-Organizing Is Not Self-Managing: A Case Study About Governance Challenges in an Agile IT Unit and Its Scrum Projects*. https://doi.org/10.24251/hicss.2019.784

Surenthran, D. P., Umamaheswari, S., Blessie, P. R., Karthick, K., Nithyakarpgam, A., & Devapitchai, J. J. (2024). *Agile Sustainability Revolutionizing Risk Management in Finance*. 249–268. https://doi.org/10.4018/979-8-3693-6274-7.ch014

Tak, A., & Chahal, S. C. S. (2024). Risk Management in Agile Al/Ml Projects: Identifying and Mitigating Data and Model Risks. *Journal of Technology and Systems*, *6*(3), 1–18. https://doi.org/10.47941/jts.1824

Thom-Manuel, O. M. (2022). Explicit Risk Management in Agile Software Projects: Its Relevance and Benefits. *Asian Journal of Research in Computer Science*, 12–24. https://doi.org/10.9734/ajrcos/2022/v14i330340

Tiwari, A. (2024). Collaborative Governance and Integrated Risk Management Framework of Natural Disasters. *Journal of Asia Business Studies*, *18*(6), 1668–1686. https://doi.org/10.1108/jabs-10-2022-0342

Uwadi, M., Gregory, P., Allison, I., & Sharp, H. (2022). *Roles Of Middle Managers In Agile Project Governance*. 65–81. https://doi.org/10.1007/978-3-031-08169-9_5

Verma, P., & Tyagi, A. (2025). Agile Methodologies in Database Management: Discussing the Application of Agile Scrum and Kanban in Database Administration. *Ijrmeet*, *13*(4), 224–243. https://doi.org/10.63345/ijrmeet.org.v13.i4.13

Vieira, M., Hauck, J. C. R., & Matalonga, S. (2020). *How Explicit Risk Management Is Being Integrated Into Agile Methods: Results From a Systematic Literature Mapping*. 1–10. https://doi.org/10.1145/3439961.3439976

Vududala, S. K. (2020). Best Practices for Implementing Scrum in Jira. *International Journal of Multidisciplinary Research and Growth Evaluation*, *1*(1), 106–109. https://doi.org/10.54660/.ijmrge.2020.1.1.106-109

Wang, Z., Yao, Y., & Cai, S. (2025). Authentic leadership and employee expediency: A moderated mediation framework. *Journal of Managerial Psychology*, *ahead-of-print*(ahead-of-print). https://doi.org/10.1108/JMP-11-2023-0682

Wiedemann, A. (2018). *IT Governance Mechanisms for DevOps Teams—How Incumbent Companies Achieve Competitive Advantages*. https://doi.org/10.24251/hicss.2018.617

Wijaya, R., Kumorotomo, W., Ratminto, R., & Djunaedi, A. (2024). Government Organization Adaptation to Implement Agile Practices in Provincial Smart City Agency. *Eduvest - Journal of Universal Studies*, *4*(9), 8024–8045. https://doi.org/10.59188/eduvest.v4i9.30330