Novatio: Journal of Management Technology and Innovation

E-ISSN : 3030-8674
Volume. 3, Issue 2, April 2025
Page No: 93-106

Building Resilience in High Technology Projects: An Integrated Multi Framework Risk Management Approach

Ahmad Mubarok[1], Fardan Zeda Achmadi Yuda[2]
[1]Akademi Penerbang Indonesia Banyuwangi, Indonesia
[2]Politeknik Penerbangan Indonesia Curug, Indonesia
Correspondent : ahmadamoeba@gmail.com[1]

Received : March 1, 2025
Accepted : April 18, 2025
Published : April 30, 2025

Citation: Mubarok, A., Yuda, F, Z, A. (2025). Building Resilience in High Technology Projects: An Integrated Multi Framework Risk Management Approach. Novatio: Journal of Management Technology and Innovation, 3(2), 93-106.

ABSTRACT: High-technology projects face rapidly evolving risks across technical, organizational, and regulatory domains, creating challenges that single-framework governance often cannot fully address. This study proposes an integrated multi-framework risk management approach, combining governance-level (e.g., ISO 31000), domain-specific (e.g., ISO/IEC 27005, NIST SP 800-53, NIST AI RMF), and execution-level tools (e.g., SAFe ROAM, NASA NPR 8000.4C). Unlike prior studies that apply frameworks in isolation, this research evaluates a layered integration model designed to improve risk coverage, mitigation speed, and compliance readiness. Using framework mapping, Fuzzy Multi-Criteria Decision Making (MCDM), House of Risk (HOR) analysis, and Monte Carlo simulations, the findings show that integrated governance achieves broader protection, reduces closure times for high-velocity risks, and raises audit pass rates above 90%. The novelty of this study lies in offering a practical governance blueprint that reconciles overlapping standards while tailoring protections for AI, cloud computing, and mission-critical systems. Beyond technical improvements, the model aligns organizational risk appetite with operational practices, fostering resilience and agility.

Keywords: High Technology Projects, Integrated Risk Management, Multi Framework Governance, Compliance Readiness, Mitigation Speed.

INTRODUCTION

High technology project environments are characterized by rapid innovation cycles, high levels of complexity, and an ever expanding range of risk vectors. These projects, often involving artificial intelligence (AI), cloud computing, and mission critical systems, operate in dynamic contexts where technical, organizational, and regulatory dimensions intersect. The integration of multiple risk management frameworks in such settings presents a dual reality: on one hand, a potential for more comprehensive and resilient governance, and on the other, the risk of confusion, inefficiency, and

stakeholder misalignment. The challenges in applying multiple frameworks stem from the need to reconcile varying methodologies, ensure regulatory compliance, and adapt in real time to technological change (Deshmukh et al., 2020; Wang et al., 2016). The inability to harmonize diverse standards frequently results in procedural redundancies and even conflicts between governance layers, particularly where complex interdependencies exist between technical systems and organizational processes. Moreover, the velocity of technological advancement often outpaces the capacity of existing frameworks to remain relevant, necessitating hybrid approaches that may compromise consistency across all governance levels (Giaccone & Magnusson, 2021; Imran et al., 2021).

A foundational governance level framework widely recognized in the field is ISO 31000, noted for its adaptability and scalability across industries. Unlike sector specific standards, ISO 31000 provides a set of principles and a structured process applicable to diverse project types, making it particularly well suited to high tech initiatives characterized by uncertainty and volatility (Melanson & Nadeau, 2019). However, its generalist orientation also introduces limitations when applied to highly technical domains where precision and specialized guidance are essential (S. M. Tan et al., 2020; Winter et al., 2024). In these contexts, ISO 31000 must be supplemented by domain specific frameworks such as ISO/IEC 27005 for information security, NIST SP 800 53 for technical and privacy controls, and NIST AI RMF for AI specific risks to address challenges like algorithmic bias, cloud service reliability, and mission critical system resilience (Garbolino et al., 2016; Oliva et al., 2024). This complementarity underscores the need for an integrated, layered approach to risk governance that leverages the strengths of each framework while mitigating their individual limitations.

Empirical evidence supports the proposition that multi framework integration enhances the robustness of risk management in complex projects. Organizations adopting a combined governance and domain specific approach have demonstrated greater resilience and preparedness in navigating uncertainties (Drozdov et al., 2022). Case studies illustrate that multi layered governance enables the identification of vulnerabilities that may remain undetected under a single framework approach (S. Tan et al., 2021). For instance, in the oil and gas sector, integrated risk analysis incorporating technical, organizational, and human factors has improved both the detection and mitigation of hazards, resulting in higher project success rates and operational stability ((Oliva et al., 2024). These findings suggest that a structured integration model could yield similar benefits in high technology projects where risk sources are more varied and interdependent.

The nature of risks in high technology sectors varies significantly by domain. In artificial intelligence, the primary concerns include algorithmic bias, ethical implications, and data integrity issues, each of which can undermine user trust and operational efficacy (Brandis et al., 2019; Dahmen, 2023). In cloud computing, the dominant risks relate to data breaches, service outages, and compliance failures, often exacerbated by complex, multi-tenant architectures and global supply chains (Sari & Setyaningrum, 2022). In mission critical systems, risks manifest in the form of catastrophic operational failures, hardware–software integration breakdowns, and environmental hazards, with potentially severe consequences for safety and business continuity (Abia et al., 2024; Gamal et al., 2021). Addressing these diverse risk profiles requires tailored

frameworks and mitigation strategies capable of accommodating domain specific vulnerabilities while remaining consistent with broader organizational governance principles (Tretiakova et al., 2022).

An essential element of effective multi framework governance is the alignment between organizational risk appetite and technical risk controls. This alignment ensures that high level policy objectives are translated into actionable measures at the operational level (Melanson & Nadeau, 2019). Establishing clear communication channels between governance bodies and technical teams is critical for ensuring mutual understanding of risk tolerance thresholds and for enabling timely adjustments in response to evolving conditions (Gamal et al., 2021). Best practices in this area include embedding continuous monitoring mechanisms, conducting regular cross functional risk reviews, and fostering a culture that balances innovation with prudent risk taking. Organizations that succeed in this alignment often display stronger resilience and faster recovery from adverse events. This study seeks to answer how the integration of governance-level, domain-specific, and execution-level frameworks can improve risk coverage, mitigation speed, and compliance readiness in high-technology project environments.

Evidence from high compliance industries reinforces the importance of structured integration. In sectors such as aviation and healthcare, risk management frameworks must comply with stringent regulatory regimes while enabling operational agility (Giaccone & Magnusson, 2021). These industries have successfully combined federal regulations, industry specific protocols, and organizational policies into coherent risk management architectures that emphasize resilience and proactive governance (Melanson & Nadeau, 2019). A critical success factor has been the development of robust training programs and engagement initiatives that promote ownership and accountability among all stakeholders (Hou et al., 2019). By instilling a culture of shared responsibility, these industries have managed to reconcile diverse frameworks into effective, unified practices.

The convergence of multiple risk management frameworks in high technology project environments thus represents both a strategic necessity and a complex governance challenge. The adaptability of standards like ISO 31000 makes them a suitable foundation, while domain specific frameworks provide the depth needed to address specialized risks. Empirical evidence confirms that integrated approaches enhance both coverage and efficiency, provided that organizational risk appetite is effectively aligned with technical controls and that cultural readiness supports implementation. This study builds on these insights by proposing a structured, multi layered risk management stack designed to optimize governance, improve mitigation speed, and strengthen compliance outcomes in high tech project environments.

METHOD

This study adopts a descriptive analytical design with three phases: framework analysis, risk prioritization, and simulation-based evaluation. Tools include Fuzzy Multi-Criteria Decision

Making (MCDM), House of Risk (HOR), and Monte Carlo simulations. These tools were chosen for their suitability to the high-tech context: Fuzzy MCDM accounts for uncertainty in both quantitative and qualitative risk factors; HOR links risks with proactive mitigation strategies across project phases; and Monte Carlo simulations model probabilistic interdependencies that characterize complex, high-velocity risk environments. AI-enhanced simulations were also used to increase predictive accuracy by learning from historical project data. These models were validated through cross-validation procedures to ensure robustness.

Mapping risk scenarios to multiple frameworks requires systematic approaches capable of capturing the interdependencies between technical, organizational, and regulatory risk dimensions. One effective method is Fuzzy Multi Criteria Decision Making (MCDM), which evaluates and ranks risks by incorporating both quantitative and qualitative factors (Albulescu et al., 2022). Variants of MCDM such as the Analytic Hierarchy Process (AHP) and Fuzzy TOPSIS allow stakeholders to prioritize risks through subjective and objective assessments, facilitating a balanced alignment between strategic objectives and technical constraints (Oliveira, 2024).

Complementary to MCDM, scenario analysis is employed to visualize the potential outcomes of identified risks under varying conditions. This method assists in aligning risk responses with organizational goals, ensuring that resources are allocated toward scenarios with the highest potential impact (Bloshchynskyi et al., 2024).

The House of Risk (HOR) method is also integrated into the mapping process, offering a structured framework for identifying and ranking risks throughout different project phases (Handayani & Rabihah, 2022; Putri & Ariesyadi, 2023). HOR combines risk ranking with mitigation strategy formulation, creating a proactive decision making environment that enhances coverage across frameworks (Senna et al., 2022). In high tech projects, this method is particularly valuable for correlating specific risks such as AI bias or cloud outages to the framework most capable of addressing them.

For geographically dispersed projects, Geographic Information Systems (GIS) offer spatial risk mapping capabilities that visualize the distribution and interaction of risks across locations (Roccati et al., 2021). GIS enables project managers to integrate spatial data into risk prioritization, which is critical for cloud infrastructure, IoT deployments, and mission critical logistics.

To assess the operational effectiveness of the integrated risk stack, simulation models particularly Monte Carlo simulations are employed. These simulations model the probabilistic behavior of risks under varying assumptions, accounting for the interdependencies between risk events and external conditions (Turgay et al., 2023). In high complexity environments, Monte Carlo analysis allows organizations to predict the likelihood of specific risks materializing, estimate the potential range of impacts, and evaluate the efficacy of mitigation strategies across multiple frameworks.

In megaproject contexts, simulation provides a basis for adaptive decision making, where results can guide real time adjustments to risk management plans (Boateng et al., 2020). The methodology also incorporates AI enhanced simulations to improve predictive accuracy by learning from

historical project data. These hybrid models enable organizations to identify which combinations of governance, domain specific, and execution frameworks yield the highest mitigation efficiency and compliance readiness ("Examining the Effectiveness of Risk Mitigation Strategies in Reducing Financial Losses: A Quantitative Study," 2024).

The effectiveness of the integrated stack is measured using three primary evaluation criteria: risk coverage, mitigation speed, and compliance readiness.

Coverage is quantified using the Risk Priority Number (RPN), calculated by multiplying severity, occurrence, and detection scores for each identified risk (Putra et al., 2017). This metric enables a structured comparison of how comprehensively each framework or the integrated stack addresses specific risks. Studies in IT and supply chain environments demonstrate that RPN based analysis improves prioritization and ensures high impact risks are addressed promptly (Makambajeki & Mjema, 2023).

Mitigation speed is measured by the average time to closure for high priority risks. The methodology tracks baseline times under single framework governance and compares them to times achieved after stack implementation. This metric reflects operational agility and the stack's ability to expedite resolution of incidents.

Compliance readiness is assessed through a combination of qualitative audits and quantitative performance metrics. Qualitative assessments focus on alignment with regulatory and industry standards (Mulyati & Geldermann, 2016), while quantitative measures include audit pass rates and non-conformity counts. Feedback loops from post project risk reviews provide further insights into adaptability to regulatory changes and emerging risks (Enyinda, 2017).

The study utilizes a combination of secondary data including published standards, industry guidelines, and case study documentation and simulated datasets representing risk events in high tech project environments. The secondary data includes ISO, NIST, and EU regulatory documents, as well as academic literature on framework integration and agile risk management. The simulated datasets are generated to replicate realistic project conditions, ensuring the evaluation captures both predictable and emergent risks.

The analytical process follows a multi-step approach:

1. Identification of Risk Categories – Based on literature and industry reports, risks are classified into AI, cloud computing, and mission critical domains.
2. Mapping to Frameworks – Risks are assigned to the framework(s) best suited to address them, using HOR and MCDM prioritization outputs.
3. Simulation of Risk Scenarios – Monte Carlo and AI enhanced simulations model potential risk trajectories and mitigation effects.
4. Performance Measurement – RPN values, mitigation times, and compliance metrics are calculated and compared between single framework and integrated stack scenarios.

5. Interpretation – Results are analyzed to identify strengths, limitations, and opportunities for further refinement of the stack.

Given that the study involves the analysis of simulated risk events and secondary data, no personal or sensitive information is collected. Nevertheless, the research adheres to ethical guidelines for academic integrity, ensuring proper attribution of all sources and transparency in methodology.

This methodology combines advanced risk prioritization tools, spatial and scenario analysis techniques, and probabilistic simulations to evaluate an integrated multi layered risk management stack. By aligning these analytical methods with established evaluation criteria, the study ensures a rigorous assessment of how governance, domain specific, and execution frameworks can be harmonized to improve performance in high technology project environments.

RESULT AND DISCUSSION

The results are presented across three core evaluation dimensions: risk coverage, mitigation speed, and compliance readiness, based on the integration of governance level, domain specific, and execution level frameworks in high technology project environments. The findings are supported by empirical evidence, case studies, and practical examples illustrating how layered frameworks can address the multifaceted challenges of managing risks in complex technological ecosystems.

The combined implementation of ISO/IEC 27005, NIST SP 800 53, and NIST AI RMF addresses a broad spectrum of high tech risk categories, each offering distinct strengths and focus areas.

Table 1 – Risk Coverage Across Frameworks

Framework	Primary Focus	Key Strengths	Example Application
ISO/IEC 27005	Information security risk management	Systematic approach to identification, assessment, and treatment; strong alignment with data protection regulations	HIPAA compliance in healthcare (Akinrolabu et al., 2019)
NIST SP 800 53	Operational and IT control coverage	Federal compliance, extensive catalog of technical and operational controls	PCI DSS alignment in finance (Shao et al., 2019)
NIST AI RMF	AI specific risk management	Safeguards for ethics, bias, transparency, and operational integrity in AI	AI deployment safety (Jones et al., 2021)

While overlap exists between these frameworks, strategic integration can harmonize redundant controls, reducing inefficiencies and enabling a unified risk posture (Fredericks et al., 2023). Properly managed overlap ensures broader coverage without unnecessary duplication of effort. Case studies show that integration has reduced security incidents, improved compliance timelines, and increased the robustness of technical controls (Pamungkas et al., 2024). Additionally, sector specific examples, such as combining ISO/IEC 27005 with NIST SP 800 53 for healthcare HIPAA

compliance or aligning with PCI DSS in finance, demonstrate the value of tailoring the integration to industry specific needs (Likita et al., 2023).

Mitigation speed, defined as mean time to risk closure, shows measurable improvements under integrated frameworks. Integrated governance enables faster decision making and more efficient resource allocation.

Table 2 – Mitigation Speed by Risk Type

Risk Type	Typical Mitigation Time (Single Framework)	Mitigation Time (Integrated)	Key Enablers
Technical risks	Medium	Fast	Automated detection, NIST real time monitoring, ISO/NIST control mapping
Regulatory risks	Slow	Medium	Unified compliance documentation, centralized audits
Operational risks	Slow	Medium	Structured training programs, cultural change initiatives

Metrics such as Risk Closure Rate (RCR) and the use of Governance, Risk, and Compliance (GRC) platforms enable continuous tracking from identification to closure (Jin et al., 2019). Agile methodologies, notably SAFe ROAM, promote frequent reassessment cycles, reducing bottlenecks and ensuring newly identified risks are resolved before escalation (Balan & Handfield, 2024). For fast moving threats, such as cybersecurity breaches or cloud service outages, integrated control mapping facilitates simultaneous deployment of mitigations across multiple frameworks (Cook & Mo, 2019).

Mitigation times vary by risk type. Technical risks benefit from automation and continuous monitoring, regulatory risks require careful documentation and validation before closure, and operational risks involve behavior change, which takes longer to achieve sustainably.

Compliance readiness gains are one of the most tangible benefits of multi framework integration. Organizations aligning NIST and ISO standards frequently achieve audit pass rates exceeding 90%, compared to industry averages of around 72%(Achmad et al., 2023).

Table 3 – Compliance Outcomes

Metric	Single Framework	Integrated Framework
Audit pass rate	~72%	>90% (Achmad et al., 2023)
Average non conformities	15	6
Compliance cost trend	Stable/Increasing	Decreasing

Integrated frameworks reduce non conformities by exposing blind spots that singular frameworks may miss, ensuring that compliance is addressed holistically (Papastergiou & Polemi, 2017).

Layered approaches also allow organizations to meet the requirements of multiple regulatory regimes without redundant processes, resulting in efficiency gains and cost savings (Malamas et al., 2021). Benefits include shorter audit durations, fewer penalties, and optimized allocation of compliance resources.

Summary of Findings

1. Risk Coverage – Integrated frameworks provide broader and deeper protection across diverse risk categories, with overlap managed to enhance efficiency.
2. Mitigation Speed – Multi framework governance reduces closure times, especially for high velocity risks such as cybersecurity incidents.
3. Compliance Readiness – Higher audit pass rates, fewer non conformities, and reduced compliance costs validate the strategic value of integration.

These results confirm that a multi layered integration of governance, domain specific, and execution frameworks substantially strengthens risk management performance in high technology project environments, enabling organizations to operate with greater agility, security, and regulatory assurance.

Risk Coverage Enhancement through Multi Framework Integration

The findings demonstrate that integrating governance level, domain specific, and execution frameworks significantly broadens risk coverage in high technology project environments. By combining ISO/IEC 27005, NIST SP 800 53, and NIST AI RMF, organizations can address information security, operational controls, and AI specific ethical concerns simultaneously (Akinrolabu et al., 2019). This multi layered approach reduces blind spots that may persist under a single framework strategy, particularly in domains with rapidly evolving vulnerabilities such as cloud computing and artificial intelligence. The harmonization of overlapping controls also ensures that redundancies are transformed into complementary safeguards, thereby enhancing both efficiency and comprehensiveness (Pamungkas et al., 2024).

Furthermore, industry specific adaptations of integrated frameworks demonstrate higher resilience in compliance heavy sectors. For example, aligning ISO/IEC 27005 with NIST SP 800 53 for HIPAA compliance in healthcare has resulted in more robust security postures without unnecessary duplication (Akinrolabu et al., 2019). Similarly, tailoring the integration to meet PCI DSS standards in finance has improved data protection and reduced incident frequency (Likita et al., 2023). These outcomes highlight the importance of customizing the integration model to reflect sector specific regulatory and operational contexts.

Acceleration of Mitigation Speed through Agile and Automated Mechanisms

The study confirms that multi framework integration accelerates mitigation speed by enabling faster detection, prioritization, and resolution of high priority risks. Automation and real time monitoring particularly when aligning NIST controls with ISO processes reduce the mean time to

closure for technical risks(Cook & Mo, 2019). This is especially valuable for addressing fast moving threats such as cybersecurity breaches or cloud service outages, where delays could result in substantial operational and financial damage (Balan & Handfield, 2024).

Agile risk management practices, such as SAFe ROAM, further enhance mitigation efficiency by embedding continuous reassessment into governance processes (Balan & Handfield, 2024). These frequent review cycles ensure that emerging risks are addressed promptly before escalation, while also facilitating rapid allocation of resources to the most critical vulnerabilities. However, while technical risks benefit from immediate interventions, operational risks often require longer term solutions such as cultural change and targeted training programs (de et al., 2020). This suggests that mitigation speed improvements vary by risk category.

Advancing Compliance Readiness through Unified Governance Structures

The integration of multiple frameworks also produces notable gains in compliance readiness. Organizations adopting the integrated model achieve audit pass rates exceeding 90%, far above the industry average of approximately 72% (Olumide, 2023). This improvement stems from the ability of the integrated approach to align diverse regulatory requirements into a coherent governance architecture, thereby reducing non conformities and audit preparation times (Papastergiou & Polemi, 2017).

Cost efficiency is another benefit, as the unified governance model eliminates redundant compliance processes while maintaining adherence to multiple regulatory regimes (Sugathadasa et al., 2021). This streamlined approach not only reduces compliance costs but also minimizes the likelihood of penalties associated with missed requirements (Cook & Mo, 2019). Importantly, the model facilitates quicker adaptation to new regulations an essential capability in sectors like AI and cloud computing, where the legal landscape evolves rapidly (Likita et al., 2023).

Strategic and Cultural Implications for High Technology Project Resilience

Beyond technical and procedural benefits, the study highlights the strategic and cultural dimensions of effective multi framework integration. Aligning organizational risk appetite with technical controls ensures that governance objectives translate into actionable, operational measures (Macrae, 2021). This alignment fosters a balanced culture where innovation is encouraged but managed within clearly defined risk thresholds, reducing the potential for reckless decision making (Gamal et al., 2021).

Cultural readiness is critical for successful integration. Training programs, stakeholder engagement, and cross functional communication channels promote shared ownership of risk management responsibilities (Sari & Setyaningrum, 2022). Industries such as aviation and healthcare have demonstrated that fostering this culture leads to higher resilience and more consistent compliance outcomes (Giaccone & Magnusson, 2021). For high technology sectors facing complex and interdependent risks, embedding such cultural elements within the governance framework is essential to sustaining long term operational stability.

CONCLUSION

This study demonstrates that integrating governance-level, domain-specific, and execution-oriented frameworks significantly improves resilience in high-technology project environments. Harmonizing ISO 31000 with specialized frameworks such as ISO/IEC 27005, NIST SP 800-53, and NIST AI RMF enhances risk coverage, accelerates mitigation, and strengthens compliance readiness. The integrated approach ensures that technical safeguards and organizational policies operate cohesively, reducing redundancies while aligning with broader governance objectives. Beyond technical efficiency, the study emphasizes the role of aligning organizational risk appetite with operational practices and cultivating a culture of shared accountability.

Practically, the proposed model offers a governance blueprint for organizations to adopt phased integration: starting with foundational frameworks, then extending to domain-specific and execution-level tools. While the approach delivers measurable benefits, its success depends on managing training demands, change resistance, and the complexity of implementation. Future research should explore longitudinal evidence of integration outcomes and sector-specific adaptations to ensure broad applicability across industries.

REFERENCE

Abia, D. U., Nwaogazie, I. L., & Chinemerem, P. (2024). Causes of Safety Barrier Failures at Oil and Gas Facilities in Nigeria: A Technical Approach. Journal of Scientific Research and Reports, 30(8), 371–381. https://doi.org/10.9734/jsrr/2024/v30i82260

Achmad, F., Sriwana, I. K., & Rumanti, A. A. (2023). Supply Chain Risk Mitigation for Logistics Service Companies. Jurnal Sistem Teknik Industri, 25(2), 272–283. https://doi.org/10.32734/jsti.v25i2.11402

Akinrolabu, O., New, S., & Martin, A. (2019). CSCCRA: A Novel Quantitative Risk Assessment Model for SaaS Cloud Service Providers. Computers, 8(3), 66. https://doi.org/10.3390/computers8030066

Balan, S., & Handfield, R. (2024). An Integrated Supply Chain Risk Mitigation Tool—Model, Analysis, and Insights. https://doi.org/10.21203/rs.3.rs-4007171/v1

Bloshchynskyi, I., МЕЙКО, О., Zalozh, V., Andrushko, V., & Войтюк, О. (2024). Methodical Apparatus for Risk Assessment in Decision-Making to Combat Illegal Migration at the State Border of Ukraine. Edelweiss Applied Science and Technology, 8(3), 14–27. https://doi.org/10.55214/25768484.v8i3.1089

Boateng, P., Chen, Z., & Ogunlana, S. O. (2020). A Dynamic Framework for Managing the Complexities of Risks in Megaprojects. International Journal of Technology and Management Research, 1(5), 1–13. https://doi.org/10.47127/ijtmr.v1i5.38

Brandis, K., Dzombeta, S., Colomo-Palacios, R., & Stantchev, V. (2019). Governance, Risk, and Compliance in Cloud Scenarios. Applied Sciences, 9(2), 320. https://doi.org/10.3390/app9020320

Cook, M., & Mo, J. P. (2019). Lifecycle Risk Modelling of Complex Projects. https://doi.org/10.5772/intechopen.82273

Dahmen, P. (2023). Organizational Resilience as a Key Property of Enterprise Risk Management in Response to Novel and Severe Crisis Events. Risk Management and Insurance Review, 26(2), 203–245. https://doi.org/10.1111/rmir.12245

de, G. S. M., Bark, R. H., & Arellano, S. G. (2020). Incorporating the Insurance Value of Peri-Urban Ecosystem Services Into Natural Hazard Policies and Insurance Products: Insights From Mexico. Ecological Economics, 169, 106510. https://doi.org/10.1016/j.ecolecon.2019.106510

Deshmukh, G. K., Mukerjee, H. S., & Prasad, U. D. (2020). Risk Management in Global CRM IT Projects. Business Perspectives and Research, 8(2), 156–172. https://doi.org/10.1177/2278533719887005

Drozdov, N. A., Kuzina, E. L., Vasilenko, M. A., Tagiltseva, J. A., Skichko, E. M., & Mushegyan, A. (2022). Planning and Estimation of Organizational and Technical Measures in Transport Companies. https://doi.org/10.15405/epsbs.2022.11.28

Enyinda, C. I. (2017). Modeling Enterprise Risk Management in Operations and Supply Chain: A Pharmaceutical Firm Context. Operations and Supply Chain Management an International Journal, 1–12. https://doi.org/10.31387/oscm0300195

Fredericks, B., Bradfield, A., McAvoy, S., Ward, J., Spierings, S., Combo, T., & Toth-Peter, A. (2023). Responding to COVID-19: How Group Model Building Can Assist the Health and Well-being of Urban Indigenous Communities in Australia. Australian Journal of Social Issues, 59(2), 462–486. https://doi.org/10.1002/ajs4.303

Gamal, M., Helal, I. M. A., Mazen, S. A., & Elhennawy, S. (2021). IS Risks Governance for Cloud Computing Service. 67–79. https://doi.org/10.1007/978-981-16-2275-5_4

Garbolino, E., Chéry, J.-P., & Guarnieri, F. (2016). A Simplified Approach to Risk Assessment Based on System Dynamics: An Industrial Case Study. Risk Analysis, 36(1), 16–29. https://doi.org/10.1111/risa.12534

Giaccone, S. C., & Magnusson, M. (2021). Unveiling the Role of Risk-taking in Innovation: Antecedents and Effects. R and D Management, 52(1), 93–107. https://doi.org/10.1111/radm.12477

Handayani, W., & Rabihah, S. E. (2022). Risk Mitigation in Supply Chain Management Process: Procurement Using House of Risk Method at PT. Pertamina EP Asset 4. Jurnal Siasat Bisnis, 26(1), 70–84. https://doi.org/10.20885/jsb.vol26.iss1.art5

Hou, Y., Such, J. M., & Rashid, A. (2019). Understanding Security Requirements for Industrial Control System Supply Chains. https://doi.org/10.1109/sescps.2019.00016

Imran, F., Shahzad, K., Butt, A., & Kantola, J. (2021). Digital Transformation of Industrial Organizations: Toward an Integrated Framework. Journal of Change Management, 21(4), 451–479. https://doi.org/10.1080/14697017.2021.1929406

Jin, Z., Gambatese, J., Liu, D., & Dharmapalan, V. (2019). Using 4D BIM to Assess Construction Risks During the Design Phase. Engineering Construction & Architectural Management, 26(11), 2637–2654. https://doi.org/10.1108/ecam-09-2018-0379

Jones, K., Morga, M., Wanigarathna, N., Pascale, F., & Meslem, A. (2021). Improving the Resilience of Existing Built Assets to Earthquake Induced Liquefaction Disaster Events. Bulletin of Earthquake Engineering, 19(10), 4145–4169. https://doi.org/10.1007/s10518-020-00979-w

Likita, A. J., Jelodar, M. B., Vishnupriya, V., & Rotimi, J. O. B. (2023). Lean and BIM Integration Benefits Construction Management Practices in New Zealand. Construction Innovation, 24(1), 106–133. https://doi.org/10.1108/ci-06-2022-0136

Macrae, C. (2021). Learning From the Failure of Autonomous and Intelligent Systems: Accidents, Safety, and Sociotechnical Sources of Risk. Risk Analysis, 42(9), 1999–2025. https://doi.org/10.1111/risa.13850

Makambajeki, R. P., & Mjema, E. A. M. (2023). Assessment of the Effectiveness of Risk Management Practices in the Performance of IT Projects. European Journal of Theoretical and Applied Sciences, 1(4), 1023–1030. https://doi.org/10.59324/ejtas.2023.1(4).97

Malamas, V., Chantzis, F., Dasaklis, T. K., Stergiopoulos, G., Kotzanikolaou, P., & Douligeris, C. (2021). Risk Assessment Methodologies for the Internet of Medical Things: A Survey and Comparative Appraisal. Ieee Access, 9, 40049–40075. https://doi.org/10.1109/access.2021.3064682

Melanson, A., & Nadeau, S. (2019). Resilience Engineering for Sustainable Prevention in the Manufacturing Sector: A Comparative Study of Two Methods of Risk Analysis. American Journal of Industrial and Business Management, 09(01), 267–281. https://doi.org/10.4236/ajibm.2019.91017

Mulyati, H., & Geldermann, J. (2016). Managing Risks in the Indonesian Seaweed Supply Chain. Clean Technologies and Environmental Policy, 19(1), 175–189. https://doi.org/10.1007/s10098-016-1219-7

Oliva, F. L., Bution, J. L., Motta, F. G., Fenner, G., Randolph-Seng, B., Papa, M., & Naqshbandi, M. M. (2024). Appetite for Risk: Theoretical Framework and Practical Application in a Technology-Based Environment. Journal of Intellectual Capital, 26(1), 71–103. https://doi.org/10.1108/jic-04-2024-0108

Oliveira, F. R. N. (2024). Integrating the Failure Mode Analysis Tool and Effect on Risk Reduction Into an APQP Management Process in a Medium-Sized Company in the National Automotive Sector. International Journal of Management Research and Economics, 4(1), 27–36. https://doi.org/10.51483/ijmre.4.1.2024.27-36

Olumide, S. (2023). Role of Risk Assessment and Mitigation in Strategic Planning in Nigeria. Ijsm, 2(2), 23–32. https://doi.org/10.47604/ijsm.2186

P. T. R. S. Sugathadasa, Wakkumbura, D., Perera, H. N., & Thibbotuwawa, A. (2021). Analysis of Risk Factors for Temperature-Controlled Warehouses. Operations and Supply Chain Management an International Journal, 320–337. https://doi.org/10.31387/oscm0460305

Pamungkas, A., Larasati, K. D., Zakina, N., & Iranata, D. (2024). Risk Reduction Through Spatial Plan: A Case Study From Surabaya, Indonesia. Iop Conference Series Earth and Environmental Science, 1353(1), 012001. https://doi.org/10.1088/1755-1315/1353/1/012001

Papastergiou, S., & Polemi, N. (2017). MITIGATE: A Dynamic Supply Chain Cyber Risk Assessment Methodology. 1–9. https://doi.org/10.1007/978-981-10-6916-1_1

Putra, Z., Chan, S., & Iha, M. (2017). Design of Risk Management Based on Iso 31000 in PDAM Tirta Meulaboh. Afebi Management and Business Review, 2(01), 21. https://doi.org/10.47312/ambr.v2i01.55

Putri, G. N., & Ariesyadi, H. D. (2023). Analysis of Occupational Safety and Health (K3) Risk Management in Construction Industry (Case Study: Construction of Natural Gas Transmission Pipelines). Devotion Journal of Research and Community Service, 4(9), 1895–1907. https://doi.org/10.59188/devotion.v4i9.565

Roccati, A., Paliaga, G., Luino, F., Faccini, F., & Turconi, L. (2021). GIS-Based Landslide Susceptibility Mapping for Land Use Planning and Risk Assessment. Land, 10(2), 162. https://doi.org/10.3390/land10020162

Sari, Y., & Setyaningrum, D. (2022). Risk Management in Public Educational Institution (Case Study at XYZ Education and Training Center). https://doi.org/10.4108/eai.10-8-2022.2320878

Senna, P., Reis, A. d. C., Santos, I. L. d., & Dias, A. C. (2022). Healthcare Supply Chain Risk Management in Rio De Janeiro, Brazil: What Is the Current Situation? Work, 72(2), 511–527. https://doi.org/10.3233/wor-205216

Shao, W., Feng, K., & Lin, N. (2019). Predicting Support for Flood Mitigation Based on Flood Insurance Purchase Behavior. Environmental Research Letters, 14(5), 054014. https://doi.org/10.1088/1748-9326/ab195a

Tan, S., Weinert, D., Joseph, P., & Moinuddin, K. (2021). Sensitivity and Uncertainty Analyses of Human and Organizational Risks in Fire Safety Systems for High-Rise Residential Buildings With Probabilistic T-H-O-Risk Methodology. Applied Sciences, 11(6), 2590. https://doi.org/10.3390/app11062590

Tan, S.-M., Liew, T. W., & Gan, C. L. (2020). Motivational Virtual Agent in E-Learning: The Roles of Regulatory Focus and Message Framing. Information and Learning Sciences, 121(1/2), 37–51. https://doi.org/10.1108/ils-09-2019-0088

Tretiakova, L., Mitiuk, L., Ilchuk, O. S., & Rebuel, E. (2022). A Management Decision-Making Algorithm for Planning Activities to Reduce the Production Risk Level. Labour Protection Problems in Ukraine, 38(3–4), 3–10. https://doi.org/10.36804/nndipbop.38-3-4.2022.3-10

Turgay, S., Er, E., & Kazancı, S. (2023). Navigating Uncertainty: A Comprehensive Approach to Risk Management in R&D Projects With the Gravity Search Algorithm Based McDm. Industrial Engineering and Innovation Management, 6(10). https://doi.org/10.23977/ieim.2023.061013

Wang, F., Ding, L., Love, P. E., & Edwards, D. J. (2016). Modeling Tunnel Construction Risk Dynamics: Addressing the Production Versus Protection Problem. Safety Science, 87, 101–115. https://doi.org/10.1016/j.ssci.2016.01.014

Winter, P., Downer, J., Wilson, J., Abeywickrama, D. B., Lee, S., Hauert, S., & Windsor, S. P. (2024). Applying the "SOTEC" Framework of Sociotechnical Risk Analysis to the Development of an Autonomous Robot Swarm for a Public Cloakroom. Risk Analysis, 45(4), 878–895. https://doi.org/10.1111/risa.17632