ISSN: 0975-833X

Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 18, Issue, 08, pp.38061-38066, August, 2026
DOI: https://doi.org/10.24941/ijcr.50702.08.2026

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

RESEARCH ARTICLE

THE IMPACT OF RISK BREAKDOWN STRUCTURE (RBS) ON MANAGING COMPLEX TECHNOLOGY PROJECTS IN THE TELECOMMUNICATIONS AND INFORMATION TECHNOLOGY SECTOR

Faisal Ghannam A Alshammari

PhD. Researcher in Business Administration, Regional Director of Business Development, Modern Technology Company, Riyadh, Saudi Arabia

ARTICLE INFO

Article History:
Received 17th May, 2026
Received in revised form
20th June, 2026
Accepted 27th July, 2026
Published online 31st August, 2026

Keywords:
Risk Breakdown Structure (RBS); Complex Technology Projects; Telecommunications and Information Technology Sector (Telecom & IT); Project Risk Management; Digital Transformation Projects; Cybersecurity Risks; Enterprise Resource Planning (ERP).

**Corresponding author:*
Faisal Ghannam A Alshammari

ABSTRACT

Telecommunications and information technology (IT) is one of the most hazardous project environments in today's digital economy. The projects include 5G network deployment, cloud migration, enterprise resource planning (ERP) implementation, and digital transformation initiatives, all of which are highly complex in nature, involve multiple stakeholders with interdependencies, and are subject to the ever-changing nature of cyber threats. In spite of this, very little theoretical attention has been focused on the Risk Breakdown Structure (RBS) which is hierarchically structured and categorises project risks based on their origin, in telecommunications and IT contexts. This study involves a critical and systematic review of literature that has been published in the peer reviewed journals, project management standards and sector-specific reports from 2002 to 2025. The evolution of project risk management; RBS definitions, frameworks and limitations; characteristics of complex technology projects; the telecom and IT risk environment; theoretical relationship between RBS and better project outcomes; and gaps in the existing research are all explored in six thematic areas. The study proposes that RBS provides a scalable, structured, and standards-based approach to enhance the visibility of risk, to facilitate the systematic categorisation of risk, and to facilitate informed decision-making. It also illustrates that there is no validated, sector-specific RBS framework yet available in telecommunications and IT, which is a great opportunity for further research. Theoretically, the study advances the academic discourse on structured risk management. From a practical perspective, it offers a solid justification for the adoption of RBS in technology-rich contexts for project managers and risk officers.

Citation: **Faisal Ghannam A Alshammari.** ***2026.*** "The Impact of Risk Breakdown Structure (RBS) on Managing Complex Technology Projects in the Telecommunications and Information Technology Sector". ***International Journal of Current Research, 18, (08), 38061-38066.***

INTRODUCTION

Project management in the telecommunications and IT industry is drastically changing with the growth and spread of digital infrastructure, the constantly increasing threat of cybersecurity, and the transformation of the business model due to technology. The risk environment in which organisations are operating on next-generation networks, moving legacy systems to cloud platforms or undertaking enterprise-scale digital transformation programmes is one of exceptional risk density and interdependency (Ackah & Arthur, 2025; Al-Janabi, Jabbar & Syms, 2024). These risks are not limited to just technical or operational, organisational or regulatory, geopolitical or cybersecurity; they are all multidimensional and can interact simultaneously, with cascading interactions that are inadequately represented in a conventional flat risk register. Although there are several frameworks for risk management, like the project management body of knowledge guide (PMBOK Guide), the ISO 31000:2018, a structured risk management process lacks tools adapted to the unique risk complexity of telecommunications and IT projects (Vargas, 2022). A promising approach is the Risk Breakdown Structure (RBS) proposed by Hillson (2002) as a source-based hierarchical classification of project risks. The RBS is similar to the Work Breakdown Structure (WBS) in scope management in that it breaks project risk exposure into identifiable, categorisable and prioritised pieces. It was proven to be specially applicable in IT organisations by Holzmann and Spiegler (2011) and Yu et al. (2023) in the context of 5G construction risk assessments but no further theoretical synthesis has been published that connects RBS with complex telecommunications and IT project management. This study fills this gap with a methodically conducted thematic literature review.

RESEARCH OBJECTIVES

- To critically analyse and summarise the development and understanding of RBS in project management literature.

- To analyse the main properties and risk issues involved in complex technology projects in telecommunications and IT.
- To understand the way RBS identifies, classifies and prioritises risk in complex technology situations.
- To explore, theoretically, the role application of RBS plays in enhancing project management results.
- To acknowledge the gaps in research and suggest future empirical research directions for RBS in technology intensive projects.

Research Problem: Technical complexity, regulatory pressure, escalation of cybersecurity, and rapid technological change (Radu & Amon, 2021; Yu et al., 2023) are all challenges that are distributed to telecommunications and IT projects simultaneously. The current risk management approaches in the sector mainly rely on generic risk management models developed for construction or general project environments, which are not specific to the multi-domain risk environment of 5G deployment, cloud ERP and digital transformation programmes (Holzmann & Spiegler, 2011; Ghodosi et al., 2025). Andrade and Sadaoui (2021) have suggested the RM3 framework to manage IT project risk, however the framework does not offer the visual hierarchical classification of RBS that assists in improving risk communication and alignment of stakeholders. This has resulted in organisations still having only incomplete risk identification, disorganised categorisation and reactive risk responses, rather than proactive ones, continuing to contribute to the high failure rates of technology projects worldwide.

Research Value

Theoretical Contribution: This study contributes to the theoretical literature on RBS by placing it in the context of the telecommunications and IT industry, which has not yet been structured with RBS research. The study brings together key concepts from project risk management theory, information security, digital transformation and telecommunications engineering to form a unified conceptual framework that integrates the concepts of RBS, risk visibility, source-level categorisation and comparative risk analysis for technology programmes.

Practical Contribution: In practice, the study provides a theoretically supported approach to the adoption of RBS-based practices to project managers, risk officers and technology programme directors. The sector-specific RBS outlined in table 1 can directly help to enhance the quality of risk registers, planning precision, and decision-making processes in complex technology contexts like deploying 5G infrastructure and implementing cloud ERP systems.

Research Questions

- What is the RBS and how has it evolved across project management literature?
- What principal characteristics and risk factors define complex technology projects in telecommunications and IT?
- How does RBS contribute to risk identification, categorisation, and prioritisation in complex project environments?
- How can RBS theoretically support improved project outcomes in telecommunications and IT?
- What research gaps exist regarding RBS in technology-intensive environments, and what future directions are warranted?

RESEARCH METHODOLOGY

The design of this study is a theoretical desk research design and critical systematic literature review. The sources selected were peer-reviewed articles in Scopus and Web of Science, papers from the PMI conferences, international standards (PMBOK Guide; ISO 31000:2018), and reliable sector reports. Time covered is 2002-2025, with particular focus on publications from 2020-2025. Some of the foundational contributions from before 2020 were used for continuity of the theory, in particular Hillson (2002) and Holzmann and Spiegler (2011). No empirical data collection, surveys or statistical analysis were done.

Research Limitations

This study does not draw on any tacit knowledge or unpublished experience of the practitioners, but only on published secondary sources. There is no attempt at empirical testing of theoretical propositions. Not all elements of the new risk environment can be detected in the published literature base as the field of AI and 6G is constantly evolving. The findings are relevant to the telecom industry and IT and may need to be adapted for use in other industries.

LITERATURE REVIEW

Evolution of Project Risk Management: Risk management for the projects is not something that has happened in the last decade, but rather has been a gradual shift towards structured and standards-based disciplines in the past few decades. The PMBOK Guide standardised iterative risk management processes identification, qualitative and quantitative analysis, response planning and monitoring; ISO 31000:2018 brought risk governance to the enterprise level. Vargas (2022) showed what is important about the two approaches: PMBOK uses project deliverables and process inputs/outputs to focus on risk management while ISO 31000 is used for all activities related to the organisation. This distinction matters particularly for telecommunications organisations, where project risks frequently intersect with enterprise-level exposures including cybersecurity threats and regulatory change. Based on ISO 31073:2022, Cretu (2025) continued to state that in the modern world, risk identification is not enough, it should also be documented systematically in a hierarchical format so that it can be continuously reassessed. Kiral (2025) evaluated four structured identification methods, Delphi, the Nominal Group Technique, the HAZOP and Preliminary Hazard Analysis, and noted that the selection of the method should match the complexity of the project and the number of disciplines involved, a factor which is relevant to multi-domain telecom projects. The shift towards integrated and hierarchical risk response frameworks in the field, as observed by Ghodosi et al. (2025) in the analysis of 284 scholarly sources, further supports the adoption of RBS.

Table 1. Proposed RBS Framework for Telecommunications and IT Projects (Synthesised from Hillson, 2002; Holzmann & Spiegler, 2011; Yu *et al*., 2023; Al-Janabi *et al*., 2024)

LEVEL 0	LEVEL 1	LEVEL 2	LEVEL 3
Project Risk	Technical	Infrastructure & Integration	Network failures, cloud gaps, API mismatches, legacy system conflicts
	Technical	Cybersecurity	Data breaches, ransomware, zero-day exploits, misconfigured cloud storage
	Operational	Resource & Schedule	Skill shortages, cost overruns, timeline compression, vendor delays
	Operational	Regulatory Compliance	Spectrum licensing, data governance, GDPR, telecom regulatory changes
	Organizational	Change & Governance	Stakeholder resistance, unclear project ownership, digital capability gaps
	External	Market & Geopolitical	Technology disruption, vendor concentration risk, supply chain instability

Risk Identification → Risk Categorization → RBS Construction → Risk Prioritization → Response Planning

Figure 1. RBS Process Flow for Complex Technology Projects (Adapted from Hillson, 2002; PMBOK Guide; ISO 31000:2018)

Table 3. Risk Category Framework for the Telecommunications and IT Sector (Synthesised from Ackah & Arthur, 2025; Al-Janabi *et al*., 2024; Yu *et al*., 2023; Radu & Amon, 2021)

Technical Risks	Operational Risks	Cybersecurity Risks	Strategic Risks
5G/6G deployment complexity	Resource & budget overruns	Data breach & ransomware	Digital transformation pace
Legacy system migration	Schedule compression	API exposure vulnerabilities	Technology disruption
Cloud architecture failures	Regulatory non-compliance	Supply chain attacks	Market competition shifts
Network security gaps	Vendor management failures	IoT security failures	Stakeholder misalignment

Table 1. Comparative Literature Summary RBS and Risk Management in Telecommunications and IT Projects

Author & Year	Context	Key Contribution	Relevance to RBS in Telecom/IT
Hillson (2002)	General project management	Foundational RBS definition: source-oriented hierarchical risk grouping aligned with WBS	Establishes core RBS framework applicable to all industries including telecom
Holzmann & Spiegler (2011)	Information technology organizations	IT-specific RBS across technical, organizational, management and external categories	Most directly applicable RBS model to telecommunications and IT environments
Ackah & Arthur (2025)	Telecommunications, Ghana	Quantitative study: risk assessment, control, and contingency planning positively affect project performance	Empirically validates structured risk management impact in telecom sector
Al-Janabi, Jabbar & Syms (2024)	IT project management	CYBITJET framework integrating cybersecurity into IT project lifecycle	Confirms need for structured cybersecurity risk categorization within RBS
Yu et al. (2023)	5G construction projects	Literature-Delphi model identifying 27 risk indicators across 4 dimensions	Operationalizes RBS-type hierarchical risk taxonomy in 5G telecom projects
Andrade & Sadaoui (2021)	IT project management	RM3 framework: complexity analysis, risk analysis, monitoring and control	Supports complexity-driven IT risk management; complementary to RBS approach
Vargas (2022)	Standards comparison	Parallel analysis of ISO 31000:2018 and PMBOK showing complementary risk governance	Contextualizes RBS within both ISO 31000 and PMBOK governance frameworks
Bu et al. (2024)	Digital transformation	FMEA and grey-DEMATEL applied to DT risk quantification and ranking	Risk categorization methodology transferable to RBS construction in IT projects
Radu & Amon (2021)	5G infrastructure governance	Risk-based governance for 5G deployment under geopolitical uncertainty	Demonstrates multi-dimensional telecom risk complexity requiring RBS-level structure
Cretu (2025)	Large-scale projects	Methodological foundations of risk register development using ISO 31073:2022	Bridges risk register practice with hierarchical RBS methodology for mega-projects

Complex Telecom & IT Projects (Risk Environment) ⟹ RBS Application (Risk Categorization & Prioritization) ⟹ Enhanced Risk Visibility & Informed Decisions ⟹ Improved Project Outcomes

Figure 2. Conceptual Model RBS Impact Pathway in Telecommunications and IT Complex Project Management (Authors' synthesis from reviewed literature)

Table 1. Comparative Literature Summary RBS and Risk Management in Telecommunications and IT Projects

Author & Year	Context	Key Contribution	Relevance to RBS in Telecom/IT
Hillson (2002)	General project management	Foundational RBS definition: source-oriented hierarchical risk grouping aligned with WBS	Establishes core RBS framework applicable to all industries including telecom
Holzmann & Spiegler (2011)	Information technology organizations	IT-specific RBS across technical, organizational, management and external categories	Most directly applicable RBS model to telecommunications and IT environments
Ackah & Arthur (2025)	Telecommunications, Ghana	Quantitative study: risk assessment, control, and contingency planning positively affect project performance	Empirically validates structured risk management impact in telecom sector
Al-Janabi, Jabbar & Syms (2024)	IT project management	CYBITJET framework integrating cybersecurity into IT project lifecycle	Confirms need for structured cybersecurity risk categorization within RBS
Yu et al. (2023)	5G construction projects	Literature-Delphi model identifying 27 risk indicators across 4 dimensions	Operationalizes RBS-type hierarchical risk taxonomy in 5G telecom projects
Andrade & Sadaoui (2021)	IT project management	RM3 framework: complexity analysis, risk analysis, monitoring and control	Supports complexity-driven IT risk management; complementary to RBS approach
Vargas (2022)	Standards comparison	Parallel analysis of ISO 31000:2018 and PMBOK showing complementary risk governance	Contextualizes RBS within both ISO 31000 and PMBOK governance frameworks
Bu et al. (2024)	Digital transformation	FMEA and grey-DEMATEL applied to DT risk quantification and ranking	Risk categorization methodology transferable to RBS construction in IT projects
Radu & Amon (2021)	5G infrastructure governance	Risk-based governance for 5G deployment under geopolitical uncertainty	Demonstrates multi-dimensional telecom risk complexity requiring RBS-level structure
Cretu (2025)	Large-scale projects	Methodological foundations of risk register development using ISO 31073:2022	Bridges risk register practice with hierarchical RBS methodology for mega-projects

Table 2. RBS vs. Conventional Risk Management Comparative Analysis for Telecommunications and IT

Criterion	Conventional Approach	RBS Approach	Telecom/IT Implication
Structure	Flat risk registers or simple probability-impact matrices	Hierarchical multi-level decomposition by risk source	Enables domain-specific risk taxonomy for multi-layered telecom environments
Risk Visibility	Broad groupings; limited source traceability	Granular decomposition from Level 0 to Level 3 by source	Critical for 5G, cloud, and ERP projects with overlapping risk domains
Identification Scope	Reactive; typically post-planning identification	Proactive; structured identification from project inception	Prevents overlooked risks in complex digital transformation programmes
Standards Alignment	Partial; varies by practitioner	Explicitly recommended in PMBOK Guide and aligned with ISO 31000:2018	Provides regulatory-compliant risk governance for telecommunications projects
Complexity Handling	Insufficient for multi-domain megaprojects	Scales hierarchically with increasing project complexity	Essential for managing multi-vendor, multi-domain telecom infrastructure
Cybersecurity Coverage	Generic; treated as a single risk category	Dedicated category with sub-levels for attack type, system, and impact	Addresses escalating cybersecurity risks in cloud IT and 5G telecom projects

Risk Breakdown Structure Definitions, Frameworks, and Limitations: The RBS was formally presented as a source-based categorization and definition of total risk exposure hierarchically, from a high-level down to a more specific level, by Hillson (2002) in one of his landmark conference papers of PMI. Hillson has confirmed that a well-designed RBS can help to identify all the risks, develop the right response(s), compare across projects and create a structured repository for lessons learned. This foundational work was significantly extended by Holzmann and Spiegler (2011), who developed the first IT-specific RBS and identified risks that are unique to IT projects: requirements volatility, integration complexity, vendor dependency, and cybersecurity exposure. Their framework, organised across technical, organisational, management, and external dimensions, established the principle that RBS must be calibrated to sector-specific risk topographies. RBS is a recommended risk identification tool in the PMBOK Guide and the risk principles of governance as outlined in ISO 31000:2018 provide a structured approach to the identification of risks, including a systematic approach, risk categorisation and a hierarchy analysis, which are important for effective construction of RBS. Evidence from the scholarly community also highlights areas of weakness: Construction of RBS requires domain expertise and requires building the buy-in of stakeholders, which makes it hard to be adopted by organisations with limited project maturity; and frameworks developed for a single project type may not be applicable without modification. For telecommunications and IT, this further reiterates the need for a sector-specific RBS, as discussed theoretically in table 1 below.

Complex Technology Projects Characteristics and Failure Dynamics: Al-Janabi, Jabbar and Syms (2024) recognized the complexity of an IT project to be a multi-dimensional phenomenon with five dimensions: Technical depth, Integration breadth, Stakeholder multiplicity, Regulatory density, Cybersecurity exposure, which are non-linearly amplified. While they presented a vulnerability as a cybersecurity risk, it could also be a technical risk or a compliance risk, and it could be a reputational risk, and this is a single-domain risk management approach that's invalid. After synthesizing the existing literature on IT project management over the past few decades, Andrade and Sadaoui (2021) identified that a significant part of IT projects do not meet their cost, schedule, and scope requirements, and projects with higher complexity indices need more granular and dynamic risk management practices, thus indirectly supporting RBS's hierarchical decomposition capability. Ali et al. (2024) documented the emergence of novel cloud-specific attack surfaces including misconfigured storage, insecure APIs, and insufficient access management that resist categorization within generic risk registers, which further underscores the need for a more structured approach to RBS development for each specific domain. Based on the theory of organizational

adaptation cycle, Bu et al. (2024) found that the coexistence of legacy systems and digital systems in transformation can generate special risk interactions, which cannot be effectively handled by a simple single-level risk management. Figure 1, illustrates the RBS construction process applicable to complex technology projects.

Risk Environment in Telecommunications and IT: The telecommunications industry is exposed to a very special and compound risk environment as it is undergoing transformation of its network infrastructure, it is transforming digital services, and its exposure to cybersecurity is growing. Silakova and Nikishina (2021) documented how telecom operators are transitioning their business model from traditional communication service providers to full digital service platforms a transition that introduces overlapping technical, organisational, and market risks. Radu and Amon (2021) showed that 5G infrastructure governance also faces technical uncertainties such as spectrum allocation, densification of antennas and network slicing, as well as geopolitical issues such as vendor concentration risk and national security concerns, and that it is necessary to have a multi-layer, structured governance approach to tackle these risks. Based on the systematic review by Tummala et al. (2025), the infrastructure investment needs, energy consumption, regulatory challenges, as well as the integration of legacy systems are exceptional project complexities in 5G environments. Yu et al. (2023) took this complexity one step further, and they empirically identified 27 risk indicators for a 4-dimensional taxonomy of a 5G construction project, which is very close to a sector-specific RBS. Ackah and Arthur (2025) provided critical empirical evidence: using multiple regression on data from 113 Ghanaian telecommunications managers, they established that risk assessment, risk control, and contingency planning each independently and positively predict project performance which supports the resource-based view that structured risk management is an organisation capability that provides competitive advantage. Table 3 presents an overview of the main risk categories in the telecommunications and IT sector.

Theoretical Relationship Between RBS and Complex Technology Project Management: There are three interrelated mechanisms from reviewed literature that reveal the theoretical relationship between RBS application and improved outcomes in complex technology projects. The first is risk visibility; Hillson (2002) found that risk visibility in RBS can force the project team to consider risks at many levels of granularity, resulting in a lower chance of important sources being neglected, an important consideration in telecommunications-based and IT projects where risks can be found across several technical and organisational areas. Second, the quality of categorisation procedures: Holzmann & Spiegler (2011) showed that the quality of such source-level categorisation can help to raise the quality of response strategies to address the root causes of incidents instead of the downstream implications and thus improve the effectiveness of the response. Thirdly, systematic prioritisation: Cretu (2025) noted that large scale project risk registers need multi-dimensional prioritisation that considers likelihood of risk to a project and the impact of that risk on a category, and that the RBS system helps to reveal risk concentrations across different project phases and programme portfolios. In addition, the alignment of RBS with both PMBOK and ISO 31000:2018 offers a standard-compliant justification for its adoption, especially in regulated telecommunications contexts where accountability to stakeholders and regulators is a critical issue (Vargas, 2022). Tables 1 and 2 compare and contrast some of the significant literature contributions reviewed in this study and RBS with traditional methods, respectively, according to six evaluative criteria. The conceptual model was synthesised based on the review as shown in Figure 2.

Research Gaps and Future Research Directions: The literature reviewed shows that there are three important gaps. First, no published study has developed a validated, comprehensive RBS framework specifically designed for the telecommunications and IT sector. Holzmann and Spiegler (2011) developed the first IT-specific RBS framework, but this work remains outdated and needs to be updated, while Yu et al. (2023) proposes a taxonomy of threats to 5G networks that has value but is not explicitly an RBS and has not linked to other work on IT project management. Second, there is no empirical research that has directly addressed the impact of RBS implementation on project performance in a telecommunication setting. Ackah and Arthur (2025) showed that structured risk management strategies help to improve the performance of telecom projects; their study did not examine RBS specifically a gap warranting quantitative or mixed-methods research. Third, the integration of RBS with the new trends in digital project management technology risk identification aided by AI, automated risk monitoring, and cross-organizational risk benchmarking has been almost completely overlooked and is a space of considerable practical interest for technology programme managers.

CONCLUSION

This study has explored, using a systematic and critical literature review, the theoretical link between the Risk Breakdown Structure (RBS) and complex technology project management within the telecommunications and IT industry. Five main conclusions become apparent. First, RBS offers a risk categorisation framework based on hierarchy and sources, which is clearly applicable to the multi-dimensional risk environments of telecommunications and IT projects. Second, the specific nature of the telecommunications and IT industry, with its unique risks such as deployment of 5G networks, escalation of cyber risks, digital transformation risks and regulatory uncertainty, requires a structured domain-specific approach to risk management that traditional frameworks are unable to address. Thirdly, RBS is important to project management in three ways: quality of risk categorisation at source; improved visibility of risks; and multi-dimensional risk prioritisation. Fourth, RBS is aligned to, and supports, the PMBOK Guide and ISO 31000:2018, offering a standards-compatible governance business case for using RBS in telecommunications organisations. Fifth, there are important gaps in the literature, especially the lack of a sector-specific validated RBS for telecommunications and IT and the lack of an empirical investigation that correlates RBS adoption with project performance outcomes. Suggestions for future research include: testing the RBS impact on telecoms project performance; developing a validated RBS taxonomy for the telecoms sector; and investigating RBS implementation using AI. The sector-specific RBS framework proposed in Figure 1 and the conceptual model in Figure 2 offer practical starting points for project managers and risk practitioners to operationalise these findings.

REFERENCES

Ackah, D., & Arthur, O. E. (2025). Project risk management strategies and project performance of the telecommunication industry, Ghana. Dama Academic Scholarly Journal of Researchers, 10(2), 1–27.

Al-Janabi, S., Jabbar, H., & Syms, F. (2024). Cybersecurity transformation: Cyber-resilient IT project management framework. Digital, 4(4), 866–897. https://doi.org/10.3390/digital4040043

Ali, R., Khan, S., & Haider, M. (2024). Information security risk assessment methods in cloud computing: Comprehensive review. Journal of Computer Information Systems, 64(3), 312–335. https://doi.org/10.1080/08874417.2024.2329985

Andrade, P. R. M., & Sadaoui, S. (2021). RM3: A risk management framework for IT project success. In Proceedings of the 4th International Conference on Computer Science and Software Engineering (CSSE 2021), Singapore (pp. 200–205). ACM. https://doi.org/10.1145/3494885.3494922

Bu, F., Zhang, L., & Wang, Y. (2024). Risk assessment of digital transformation from the perspective of organizational adaptation cycle. In Proceedings of ICBAR 2024 (pp. 985–996). ACM. https://doi.org/10.1145/3718751.3718913

Cretu, V. G. (2025). Methodological foundations of risk register development for large-scale projects. American Scientific Research Journal for Engineering, Technology, and Sciences, 103(1), 51–61.

Ghodosi, M., Zeinalnezhad, M., & Kazemi, A. (2025). Bibliometric analysis for modeling in construction risk management: A literature review. Management Strategies and Engineering Sciences, 7(6), 1–10.

Hillson, D. (2002). Use a risk breakdown structure (RBS) to understand your risks. Paper presented at PMI Annual Seminars & Symposium, San Antonio, TX. Project Management Institute.

Holzmann, V., & Spiegler, I. (2011). Developing risk breakdown structure for information technology organizations. International Journal of Project Management, 29(5), 537–546. https://doi.org/10.1016/j.ijproman.2010.05.009

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

Kiral, A. (2025). Contextual evaluation of risk identification techniques for construction projects. Buildings, 15(20), 3806. https://doi.org/10.3390/buildings15203806

Project Management Institute. (2021). A guide to the project management body of knowledge (PMBOK® guide) (7th ed.). PMI.

Radu, R., & Amon, J.-M. (2021). Governance of 5G infrastructure: Between path dependency and risk-based approaches. Journal of Cybersecurity, 7(1), tyab017. https://doi.org/10.1093/cybsec/tyab017

Silakova, L. V., & Nikishina, A. (2021). Digital transformation of telecom providers management customer system: A process research and effects assessment. Journal of Engineering and Applied Sciences, 13(1), 60–67.

Tummala, V., Balagangadhar, D., & Anjaneyulu, G. V. S. (2025). A systematic review on current and future prospects of 5G communications. Cogent Engineering. https://doi.org/10.1080/23311916.2025.2547635

Vargas, R. V. (2022). Risk management: A parallel between ISO 31000 (2018) and the PMBOK guide (2017). In Proceedings of the International Conference on Industrial Engineering and Operations Management, Istanbul, Turkey (pp. 1474–1483). IEOM Society International.

Yu, Z., Zhang, H., & Li, X. (2023). Managing risks in main equipment projects for 5G construction: A case study based on techno-environment-economic-planning indicator framework. Wireless Networks, 29, 3511–3528. https://doi.org/10.1007/s11276-023-03511-5

****