RESEARCH ARTICLE

SAMRIDDHI Volume 8, Issue 2, 2016 Print ISSN: 2229-7111 Online ISSN: 2454-5767

A Comparative Analysis of Risk Management Frameworks in Enterprise IT Projects

Venkata Krishna Bharadwaj Parasaram[1], Satish Kumar Nalluri[2]

[1]Graduate Researcher, Southern New Hampshire University, USA

[2]Independent Researcher, USA

ABSTRACT

Enterprise IT projects are becoming a key part of organizational strategy, and are very prone to uncertainty due to the complexity of technology, interdependence within organizations, and governance issues. Risk management is thus an important factor in enhancing the performance of the project, and balancing it with enterprise goals. This paper conducts a comparative study of the key risk management models that are implemented in the context of enterprise IT projects, their principles, structural elements, and applicability. The analysis compares project-based, enterprise-based, governance-based, and knowledge-based risk management strategies on major dimensions, which include coverage of risk, method of risk assessment, and alignment to organizational governance and the flexibility to the different degrees of project complexity. Its results show that whereas project-level frameworks are both operationally clear and responsive, they tend to be strategically disjointed at the enterprise level. On the other hand, enterprise-wide models offer the benefit of high levels of governance congruency, but can lack project-level fine-grainedness. The paper brings out the importance of hybridized risk management strategies to combine both enterprise governance arrangements and project level tooling and organizational learning systems. These types of integrated frameworks are demonstrated to be more effective when it comes to handling the multidimensional risks of the complex enterprise IT projects. The article adds to the discussion in the academic and managerial literature by providing a systematic comparative approach to informing the choice of frameworks and situational adaptation in the practice of IT risk management on an enterprise level.

Keywords: Enterprise IT projects; risk management frameworks; enterprise risk management; project risk management; IT governance; organizational risk integration.

SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology (2016); DOI: 10.18090/samriddhi.v8i2.7149

INTRODUCTION

Enterprise IT projects have become key facilitators of organizational strategy, operation integration, and competitive positioning. Enterprise resource planning systems, integrated databases and digital infrastructure projects are all large-scale systems that more and more cut across the boundary of multiple organizational departments, external vendors, and geographic locations. Although such projects are likely to deliver significant efficiency and performance improvements, they are also associated with a high degree of uncertainty, complexity as well as various types of risks exposure. It has been shown repeatedly that cost overruns, schedule slippage, and underperformance remain the enduring issues of risk management in enterprise IT project landscapes (Zwikael and Ahn, 2011).

Enterprise IT project risk is multidimensional, and includes technical, organizational, financial, strategic and psychosocial. The conventional process of risk management has been more inclined towards identifying and alleviating risks at the project level by use of tools like risk registers, qualitative assessment, and probabilistic analysis. However, comparative studies indicate that the effectiveness of these methods varies significantly in particular when they are applied to complex interdependent IT initiatives (Mileusnić Škrtica et al., 2014; Marcelino-Sadaba et al., 2014). The risk of enterprise IT projects is increasingly emanating outside the scope of the project; therefore, project-level strategies become inadequate to address those risks.

To overcome such constraints, more and more organizations have turned to enterprise risk management

Corresponding Author: Venkata Krishna Bharadwaj Parasaram, Graduate Researcher, Southern New Hampshire University, USA, e-mail: venkatakrishna.parasaram@snhu.edu

How to cite this article: Parasaram, V.K.B., & Nalluri, S.K. (2016). A Comparative Analysis of Risk Management Frameworks in Enterprise IT Projects. *SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology,* 8(2), 147-155.

Source of support: Nil

Conflict of interest: None

(ERM) systems that attempt to harmonize risk management in strategic, operational, and governance areas. ERM focuses on compatibility of risk management procedures and company goals, decision-making framework, and control mechanisms (Paape and Speklé, 2012; Rachmad, 2012). Empirical studies indicate, though, that organizational fit, governance maturity, and the degree to which enterprise level risk policies are meaningfully linked to operational and project level activities all have a significant impact on the effectiveness of ERM frameworks (Arnaboldi and Lapsley, 2014; Bromiley et al., 2015).

In the framework of enterprise IT projects, such a disjoining of project risk management and enterprise-wide risk governance is a challenging issue of paramount importance. It is suggested that knowledge-based frameworks can be utilized to fill in this gap by introducing organizational learning and historical data of projects and knowledge into IT risk management procedures (Alhawari et al., 2012). Simultaneously, the studies indicate the importance of governance systems, management skills, and the alignment of stakeholders in the process of determining the risks, distributing them, and alleviating the risks in complex projects (Guo et al., 2014; Ahsan et al., 2013). Such views suggest that the effectiveness of risk management is not only a tool and technique dependent phenomenon, but also a capability of an organization and institutional set-up.

Although there is an increasing number of articles focusing on project risk management and ERM, there is a dearth of comparison of the performance of various risk management models in the context of enterprise IT projects. Existing literature is inclined to concentrate on general project environments, non-IT sectors or at the enterprise level of governance systems without undertaking a systematic study of how these interact with each other in IT-intensive environments (Chapman, 2011; Chan et al., 2011). Moreover, the growing rise of large-scale implementation of ERP and integrated systems puts additional pressure on the necessity of consistent risk management strategies that can support both the strategic and operational implementation (Nagpal et al., 2015).

It is against this backdrop that this study is an undertaking in carrying out a comparative analysis of major risk management frameworks that apply to enterprise IT projects. The paper will attempt to elucidate the strengths, constraints, and the circumstances in which the project-centric, enterprise-wide, governance-oriented, and knowledge-based approaches can be applied. The analysis shall also add to an integrated comprehension of risk management of enterprise IT projects and shall offer conceptualization in the manner of choosing and adapting frameworks based on the requirements of the organization, project complexity and governance.

Literature Review

Conceptual Foundations of Risk Management in Enterprise IT Projects

Risk management has long been recognized as a core component of effective project management, particularly in environments characterized by uncertainty, complexity, and interdependence. Enterprise IT projects exemplify these characteristics due to their reliance on evolving technologies, cross-functional coordination, and strategic significance. Traditional project risk management literature defines risk as the effect of uncertainty on project objectives and emphasizes structured processes for risk identification, assessment, response planning, and monitoring (Zwikael & Ahn, 2011).

Comparative studies of project risk assessment methods reveal substantial variation in tools and techniques, ranging from qualitative judgment-based approaches to more formalized quantitative models. Mileusnić Škrtić and Horvatinčić (2014) demonstrate that while qualitative methods remain dominant due to their simplicity and flexibility, they often suffer from subjectivity and limited comparability across projects. These limitations become more pronounced in enterprise IT contexts, where risks frequently span organizational boundaries and extend beyond traditional project constraints.

Project Risk Management Approaches and Methodologies

Project risk management (PRM) frameworks focus on risks directly affecting project scope, schedule, cost, and quality. Empirical evidence suggests that systematic risk planning improves project outcomes across industries and national contexts, although the degree of effectiveness varies significantly depending on organizational maturity and managerial capability (Zwikael & Ahn, 2011). Marcelino-Sádaba et al. (2014) propose a structured yet adaptable PRM methodology tailored to smaller organizations, emphasizing iterative risk assessment and continuous stakeholder engagement.

In large-scale and global IT initiatives, project complexity intensifies risk exposure. Kardes et al. (2013) argue that megaproject environments require enhanced coordination mechanisms and advanced risk management capabilities to address strategic, cultural, and operational uncertainties. Within IT-specific implementations such as ERP systems, comparative analyses indicate that implementation strategy selection significantly influences risk profiles and mitigation effectiveness (Nagpal et al., 2015).

Despite their operational strengths, PRM approaches are often criticized for their limited capacity to address enterprise-wide risks, particularly those related to governance, strategic alignment, and organizational change.

Enterprise Risk Management and Organizational Integration

Enterprise risk management (ERM) emerged in response to the need for a holistic, organization-wide approach to managing risk. ERM frameworks seek to integrate strategic, financial, operational, and compliance risks into a unified governance structure. Paape and Speklé (2012) find that the adoption and design of ERM practices are shaped by firm-specific factors such as size, regulatory environment, and strategic orientation. Rather than converging toward a single best-practice model, organizations exhibit significant heterogeneity in ERM implementation.

Arnaboldi and Lapsley (2014) emphasize the importance of organizational fit in determining ERM effectiveness. Their comparative study shows that misalignment between ERM structures and existing managerial practices can reduce risk transparency and weaken accountability. Bromiley et al. (2015) further critique ERM frameworks for their tendency toward formalism, arguing that excessive emphasis on compliance and reporting may undermine proactive risk management, particularly in dynamic project environments such as enterprise IT.

From a practical perspective, ERM frameworks provide strategic coherence and governance oversight but often lack the granularity required for managing technical and project-specific risks.

Knowledge-Based and Governance-Oriented Risk Frameworks

To address the limitations of both PRM and ERM, scholars have proposed hybrid and knowledge-based risk management approaches. Alhawari et al. (2012) introduce a knowledge-based risk management framework for IT projects that leverages organizational memory, expert knowledge, and historical data to enhance risk identification and assessment. Such frameworks are particularly relevant in enterprise IT settings, where recurring technological and organizational risks can be systematically learned and anticipated.

Governance-oriented perspectives further highlight the role of formal structures, decision rights, and oversight mechanisms in shaping risk management effectiveness. Guo et al. (2014) demonstrate that well-defined governance structures improve risk communication and accountability in complex projects, although overly rigid controls may reduce adaptability. Similar insights emerge from studies of public–private partnership projects, where risk allocation and governance arrangements significantly influence project performance (Chan et al., 2011).

These perspectives suggest that effective risk management in enterprise IT projects depends not only on analytical tools but also on governance design and institutional context.

Human and Organizational Factors in Risk Management

Beyond frameworks and methodologies, the literature underscores the importance of human and organizational factors in shaping risk management outcomes. The competencies of project managers—including risk communication, leadership, and stakeholder coordination—play a critical role in translating formal frameworks into effective practice (Ahsan et al., 2013). Additionally, psychosocial and organizational risks, such as workload stress and role ambiguity, can indirectly affect IT project performance if left unaddressed (Leka et al., 2011).

These findings reinforce the view that risk management frameworks must be embedded within broader organizational and human resource systems to achieve sustained effectiveness.

Synthesis and Research Gap

The reviewed literature reveals a fragmented landscape of risk management frameworks applied to enterprise IT projects. Project-level approaches provide operational focus but insufficient strategic integration, while enterprise-wide frameworks offer governance coherence at the expense of project-level detail. Knowledge-based and governance-oriented models attempt to bridge this gap but introduce new implementation challenges related to data availability, organizational maturity, and managerial capability.

Despite extensive theoretical and empirical contributions, there remains a need for comparative analysis that systematically evaluates these frameworks within the specific context of enterprise IT projects. Addressing this gap provides the basis for understanding how different risk management approaches can be aligned and integrated to better manage the multidimensional risks inherent in enterprise IT initiatives.

METHODOLOGICAL APPROACH

This study adopts a comparative qualitative methodological approach grounded in systematic literature analysis to examine risk management frameworks applied to enterprise IT projects. The methodology is designed to facilitate structured comparison across heterogeneous frameworks while remaining sensitive to organizational, governance, and project-contextual variations. This approach is consistent with prior comparative studies in project and enterprise risk management that emphasize analytical rigor over statistical generalization (Mileusnić Škrtić & Horvatinčić, 2014; Guo et al., 2014).

Research Design

The research design is conceptual-analytical, drawing on established empirical findings, framework descriptions, and methodological critiques within the risk management literature. Rather than proposing a new framework, the study evaluates existing ones to identify patterns of convergence and divergence in their treatment of risk in enterprise IT contexts. This design is particularly appropriate given the multidimensional and context-dependent nature of IT project risk, which limits the explanatory power of single-method

empirical models (Zwikael & Ahn, 2011; Bromiley et al., 2015). The comparative design enables cross-framework evaluation at both the project level and the enterprise level, reflecting the dual governance environments in which enterprise IT projects operate (Paape & Speklé, 2012; Arnaboldi & Lapsley, 2014).

Framework Selection Criteria

- Risk management frameworks included in the analysis were selected based on four criteria:
- Relevance to enterprise IT or large-scale projects, including ERP and infrastructure-related IT initiatives
- Explicit methodological structure for risk identification, assessment, and response
- Integration with organizational governance or enterprise-wide risk processes
- Empirical or conceptual grounding in peer-reviewed literature

This selection logic aligns with established practices in comparative risk methodology research (Mileusnić Škrtić & Horvatinčić, 2014; Marcelino-Sádaba et al., 2014). Both project-centric frameworks and enterprise-wide approaches were deliberately included to capture variation in scope and governance orientation (Rachmad, 2012; Chapman, 2011).

Analytical Dimensions

Each framework was evaluated across a common set of analytical dimensions derived from prior risk management studies:

- Scope of Risk Coverage (technical, operational, strategic, organizational)
- Risk Identification and Assessment Techniques (qualitative, quantitative, knowledge-based)
- Governance and Control Mechanisms
- Organizational Integration and Fit
- Adaptability to Project Complexity and Scale

These dimensions reflect core determinants of risk management effectiveness identified in cross-industry and cross-country studies (Zwikael & Ahn, 2011; Kardes et al., 2013). Particular attention was given to governance alignment, as governance structures significantly influence risk accountability and escalation in complex projects (Guo et al., 2014).

Comparative Evaluation Procedure

The evaluation followed a three-stage procedure:

Framework Decomposition

Each framework was decomposed into its fundamental components, including risk categories, assessment tools, decision structures, and implementation mechanisms. This step supports methodological comparability across frameworks with differing terminologies and emphases (Chapman, 2011).

Cross-Framework Mapping

Framework components were mapped against the analytical dimensions to identify areas of overlap, complementarity, and divergence. This mapping approach is widely used in comparative risk studies to reduce conceptual ambiguity and enhance interpretive clarity (Chan et al., 2011; Marcelino-Sádaba et al., 2014).

Contextual Interpretation

Findings were interpreted in light of enterprise IT project characteristics, such as system integration complexity, stakeholder diversity, and organizational maturity. This step acknowledges that framework effectiveness is contingent upon contextual and human factors, including managerial competencies and risk communication capabilities (Ahsan et al., 2013; Arnaboldi & Lapsley, 2014).

Validity and Analytical Rigor

To enhance analytical rigor, the study relies on triangulation across multiple scholarly sources, combining empirical evidence, methodological critiques, and conceptual models. The use of well-established frameworks and peer-reviewed studies reduces interpretive bias and supports theoretical consistency (Bromiley et al., 2015).

While the qualitative nature of the methodology limits statistical inference, it enables deeper insight into structural and governance-related dimensions of risk management that are often underrepresented in purely quantitative studies. This trade-off is consistent with best practices in enterprise and project risk research, where contextual richness is essential for explanatory relevance (Paape & Speklé, 2012; Leka et al., 2011).

Comparative Analysis of Risk Management Frameworks

Enterprise IT projects face multifaceted risks stemming from

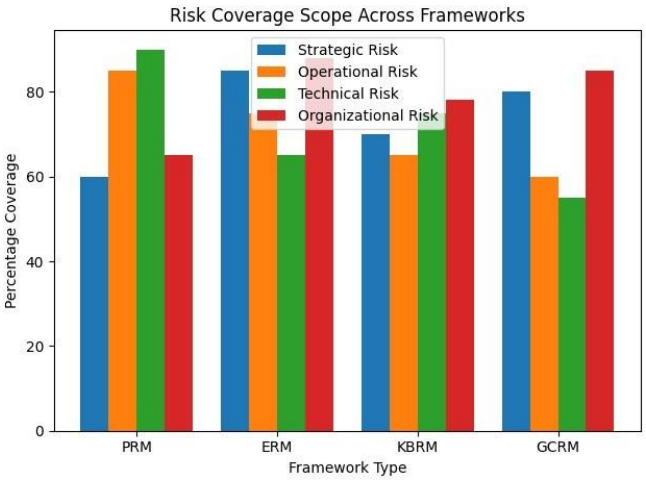

Fig 1: Illustrative comparative coverage estimates showing ERM's dominance in strategic and organizational risk domains, PRM's strength in operational and technical risk control, KBRM's balanced distribution, and GCRM's emphasis on governance-oriented oversight.

Table 1: Comparative Overview of Risk Management Frameworks

Framework Type	*Core Focus*	*Key Strengths*	*Limitations*	*Typical Application Context*
Project Risk Management (PRM)	Individual project risks	Clear structure, operational clarity, quick implementation	Limited integration with enterprise strategy	IT development projects, small-to-medium initiatives (Mileusnić Škrtić & Horvatinčić, 2014; Marcelino-Sádaba et al., 2014)
Enterprise Risk Management (ERM)	Organization-wide risk oversight	Strategic alignment, governance coherence, regulatory compliance	Less responsive to emergent project-level risks	Large enterprises, cross-functional IT programs (Arnaboldi & Lapsley, 2014; Paape & Speklé, 2012; Bromiley et al., 2015)
Knowledge-Based Risk Management (KBRM)	Leveraging organizational knowledge & historical data	Enhanced risk anticipation, promotes learning, knowledge reuse	Data-intensive, requires maturity in knowledge management	Complex IT projects, recurring system implementations (Alhawari et al., 2012; Rachmad, 2012)
Governance-Centric Risk Management (GCRM)	Oversight, escalation, and compliance	Transparency, accountability, formal control mechanisms	Can be bureaucratic and reduce responsiveness	Megaprojects, public-private partnerships, ERP implementations (Guo et al., 2014; Chan et al., 2011; Kardes et al., 2013)

Table 2: Governance Integration Across Risk Management Frameworks

Governance Dimension	*PRM*	*ERM*	*KBRM*	*GCRM*
Board / Executive Involvement	Low	High	Moderate	High
Project Autonomy	High	Moderate	Moderate	Low
Risk Escalation Clarity	Moderate	High	Moderate	Very High
Knowledge Sharing Mechanisms	Low	Moderate	High	Moderate
Formalization of Processes	Low	Moderate	Moderate	Very High

technological complexity, organizational interdependencies, and governance structures. Effective risk management frameworks must therefore balance project- level responsiveness with enterprise-wide strategic oversight. This section presents a comparative analysis of four major types of risk management frameworks Project Risk Management (PRM), Enterprise Risk Management (ERM), Knowledge-Based Risk Management (KBRM), and Governance-Centric Risk Management (GCRM) evaluated across key performance dimensions.

Comparative Framework Overview

Table 1 provides a synthesis of the core characteristics, strengths, and limitations of the four frameworks commonly applied in enterprise IT projects.

Governance and Organizational Integration

Governance integration is a critical differentiator among frameworks. ERM frameworks emphasize organizational alignment and board-level involvement, whereas PRM focuses on project team autonomy. Knowledge-based approaches rely on cross-project learning and information flows, and governance-centric approaches formalize oversight through structured escalation and reporting channels (Guo et al., 2014; Arnaboldi & Lapsley, 2014; Chapman, 2011).

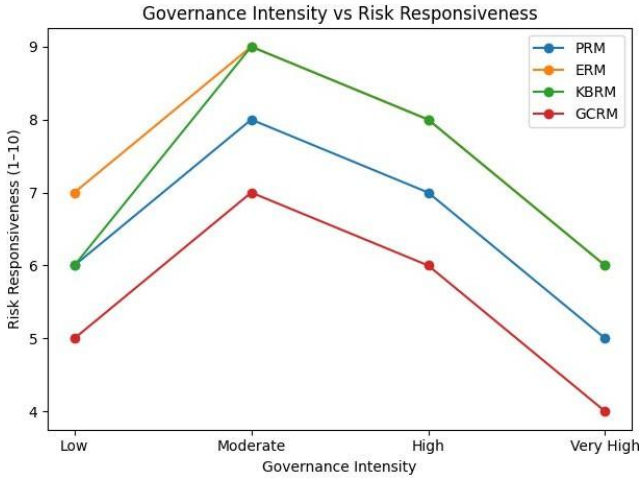

Fig 2: Conceptual relationship indicating that moderate governance intensity (ERM, KBRM) maximizes adaptive responsiveness, while excessive formalization (GCRM) may reduce agility in dynamic risk environments.

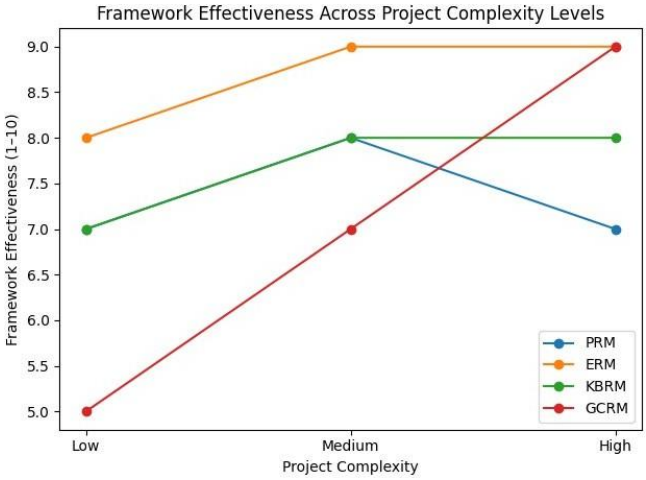

Fig 3: Theoretical performance trends suggesting hybrid ERM–PRM configurations outperform in medium-to-high complexity projects, KBRM maintains stable cross-level effectiveness, and GCRM excels primarily in high-complexity, compliance-intensive contexts.

Risk Assessment Techniques and Adaptability

Different frameworks apply distinct methodologies for risk identification, assessment, and mitigation:

PRM

Primarily uses risk registers, qualitative scoring, and probability-impact matrices (Mileusnić Škrtić & Horvatinčić, 2014; Marcelino-Sádaba et al., 2014).

ERM

Employs enterprise-wide heat maps, scenario planning, and policy-aligned risk matrices (Paape & Speklé, 2012; Bromiley et al., 2015).

KBRM

Leverages historical project data, expert knowledge bases, and predictive models for early risk detection (Alhawari et al., 2012; Rachmad, 2012).

GCRM

Uses formal escalation protocols, compliance checklists, and structured audit trails to enforce risk control (Guo et al., 2014; Chan et al., 2011).

Synthesis and Key Observations

Contextual fit matters

The effectiveness of each framework depends on organizational structure, governance maturity, and project scale (Arnaboldi & Lapsley, 2014; Kardes et al., 2013).

Hybrid approaches are optimal

Integrating ERM's strategic alignment with PRM's operational clarity and KBRM's knowledge focus enhances responsiveness and strategic coverage (Alhawari et al., 2012; Bromiley et al., 2015).

Governance intensity requires balance

Excessive formalization can reduce project agility, whereas too little oversight risks unmanaged strategic exposure (Guo et al., 2014; Chapman, 2011). This comparative analysis underscores the necessity of adaptive and hybrid risk management frameworks tailored to enterprise IT projects' complexity, scale, and organizational context.

DISCUSSION

The comparative analysis of risk management frameworks in enterprise IT projects highlights several critical insights regarding the alignment, effectiveness, and adaptability of these approaches. A key observation is that framework effectiveness is highly contingent on the context in which it is applied, including organizational size, project complexity, governance maturity, and the level of integration between enterprise and project risk management processes (Arnaboldi & Lapsley, 2014; Mileusnić Škrtić & Horvatinčić, 2014).

Project-centric frameworks excel in operational clarity, providing structured tools for risk identification, assessment, and mitigation at the project level. These approaches allow for responsive and detailed management of technical and operational uncertainties, particularly in small to medium-sized projects (Marcelino-Sádaba et al., 2014; Zwikael & Ahn, 2011). However, their primary limitation lies in their restricted scope, which often fails to account for interdependencies across projects or the strategic alignment of risks at the enterprise level (Alhawari et al., 2012).

Table 3: Risk Assessment and Adaptability Comparison

Dimension	*PRM*	*ERM*	*KBRM*	*GCRM*
Risk Identification Method	Qualitative, checklists	Enterprise-wide heat maps	Data-driven, knowledge repository	Compliance and control checklists
Adaptability to Project Complexity	High	Moderate	High	Low-Moderate
Integration with IT Governance	Low	High	Moderate	Very High
Scalability Across Projects	Moderate	High	High	Moderate

Enterprise-wide frameworks, by contrast, emphasize strategic oversight and governance integration. They facilitate alignment between project-level risk activities and broader organizational objectives, enabling consistency in decision-making and resource allocation across portfolios (Paape & Speklé, 2012; Bromiley et al., 2015). While this approach enhances transparency and accountability, it may reduce operational responsiveness due to formalized reporting structures and hierarchical risk escalation procedures (Guo et al., 2014; Rachmad, 2012).

The discussion also underscores the value of knowledge-based frameworks, which integrate organizational learning mechanisms and historical data into risk management processes. These frameworks improve risk anticipation and mitigation by allowing project managers to leverage prior experience and dynamically adapt to emerging threats (Alhawari et al., 2012; Chapman, 2011). Nevertheless, their effectiveness depends on the availability and quality of organizational knowledge assets, as well as on the competencies of personnel involved in risk identification and analysis (Ahsan et al., 2013; Kardes et al., 2013).

A recurring theme in the analysis is the role of project manager competencies in mediating the effectiveness of risk frameworks. Managers who possess strong analytical, communication, and governance skills can compensate for limitations in formal frameworks and ensure that both operational and strategic risks are adequately addressed (Chan et al., 2011; Ahsan et al., 2013).

The discussion confirms that no single framework provides a universal solution. The integration of project-level precision, enterprise-level oversight, and knowledge-based adaptability yields a hybrid risk management approach that optimally balances operational effectiveness, strategic alignment, and organizational learning. For enterprise IT projects, this integrated perspective is particularly valuable due to the complex interdependencies, technological uncertainty, and high stakes involved (Nagpal et al., 2015; Leka et al., 2011).

Implications for Enterprise IT Project Management

The comparative analysis of risk management frameworks highlights several practical implications for the management of enterprise IT projects. Organizations undertaking complex IT initiatives must recognize that risk management is not merely a procedural requirement but a strategic enabler that influences project outcomes, governance alignment, and organizational resilience.

Firstly, adopting a hybridized risk management approach that integrates project-level risk management (PRM) tools with enterprise-wide risk management (ERM) structures enhances both operational effectiveness and strategic alignment. PRM methods offer detailed risk identification, assessment, and mitigation at the project level, providing managers with actionable insights for day-to-day decision-making (Mileusnić Škrtić & Horvatinčić, 2014; Marcelino-Sádaba et al., 2014). However, without integration into an enterprise-wide framework, such approaches risk overlooking systemic and strategic exposures that may affect multiple projects or organizational objectives (Arnaboldi & Lapsley, 2014; Bromiley et al., 2015). By embedding PRM within ERM structures, organizations can ensure that risk responses are coherent across projects while remaining responsive to project-specific contingencies (Paape & Speklé, 2012; Rachmad, 2012).

Secondly, the governance context of IT projects significantly influences the effectiveness of risk management. Studies indicate that well-defined governance structures, including risk committees, reporting protocols, and escalation mechanisms, improve accountability and transparency in decision-making (Guo et al., 2014; Chan et al., 2011). However, overly rigid governance may reduce flexibility and slow response to emergent technical risks, particularly in highly complex or rapidly evolving IT projects such as ERP implementations (Nagpal et al., 2015; Kardes et al., 2013). Therefore, organizations should calibrate governance intensity to balance oversight with operational responsiveness.

Thirdly, knowledge-based and learning-oriented risk management frameworks provide significant advantages in IT project contexts. By capturing lessons learned, historical risk data, and experiential knowledge, organizations can improve predictive accuracy and enhance mitigation strategies (Alhawari et al., 2012). Integrating such knowledge mechanisms within existing risk management processes

strengthens decision-making, particularly for high-complexity projects where unforeseen risks can have substantial financial and operational impact (Zwikael & Ahn, 2011; Chapman, 2011).

Additionally, the competencies of project managers play a critical role in implementing effective risk frameworks. Recruitment and development strategies should emphasize both technical proficiency and risk management capabilities, including risk identification, stakeholder communication, and adaptive decision-making (Ahsan et al., 2013). Aligning human capital with framework requirements ensures that risk strategies are applied consistently and effectively across project lifecycles.

Finally, attention to psychosocial and organizational risk factors contributes to the overall resilience of enterprise IT projects. Incorporating elements of psychosocial risk management, such as workload balance, team dynamics, and employee well-being, supports sustainable project performance and mitigates indirect risks associated with human factors (Leka et al., 2011).

In summary, the practical implications for enterprise IT project management include:

- Integrating PRM and ERM frameworks for hybridized, context-sensitive risk management.
- Designing governance structures that provide oversight without compromising responsiveness.
- Leveraging knowledge-based approaches to enhance predictive risk management.
- Developing project manager competencies aligned with both technical and risk management requirements.
- Considering psychosocial and organizational dimensions of risk to enhance overall project resilience.

Collectively, these implications provide a roadmap for organizations seeking to optimize risk management practices in enterprise IT projects, supporting both project success and organizational strategic objectives.

Conclusion

This study provides a comprehensive comparative analysis of risk management frameworks applicable to enterprise IT projects, highlighting the unique strengths, limitations, and contextual suitability of each approach. Project risk management frameworks can be efficiently used in offering detailed operational control, in addition to responsiveness to technical uncertainty especially in small and medium-scale projects (Mileusnić Škrtica and Horvatinciaca, 2014; Marcelino-Sadaba et al., 2014; Zwikael and Ahn, 2011). They are, however, constrained by their small scope to solve strategic and organizational risks that cut across the enterprise (Arnaboldi & Lapsley, 2014; Paape and Speklé, 2012).

Enterprise-wide risk management frameworks, in their turn, provide holistic governance model and alignment to the strategy, allowing organizations to implement risk considerations in the decision-making process at all levels (Bromiley et al., 2015; Chapman, 2011; Rachmad, 2012). Such frameworks are especially useful in large and complex IT projects, such as ERP and megaproject implementation, when it is essential to coordinate the activity of multiple stakeholders and functional areas (Kardes et al., 2013; Nagpal et al., 2015). However, they may be limited in their efficacy due to the complexity of the implementation and poor project-level granularity (Guo et al., 2014; Chan et al., 2011).

Knowledge-based and hybrid solutions overcome the inconsistency between the precision of projects and the oversight of enterprises by using organizational learning, historical data, and adaptive approaches (Alhawari et al., 2012). The strategies enhance proactive risk management and ease the alignment of governance systems and operational implementation. Incorporation of the psychosocial and human resource factors also significantly increases the resiliency of the project and communication with stakeholders (Leka et al., 2011; Ahsan et al., 2013).

All in all, the discussion shows that there is no single framework which would be the best solution. Risk management within enterprise IT projects offers the need to integrate on context sensitive basis project-oriented, enterprise-wide and knowledge-based frameworks. When organizations strategically integrate these strategies, they will enjoy better mitigation of risks, better project performance and sustainable alignment with enterprise goals. Such a comparative approach can give managers and practitioners actionable insights in terms of the information on the level of risk management strategies selection, adaptation, and implementation based on the complexity and scale of enterprise IT programs.

REFERENCES

[1] Mileusnić Škrtić, M., & Horvatinčić, K. (2014). Project risk management: comparative analysis of methods for project risks assessment. *Collegium antropologicum*, *38*(1), 125-134.

[2] Arnaboldi, M., & Lapsley, I. (2014). Enterprise-wide risk management and organizational fit: a comparative study. *Journal of Organizational Effectiveness: People and Performance*, *1*(4), 365-377.

[3] Alhawari, S., Karadsheh, L., Talet, A. N., & Mansour, E. (2012). Knowledge-based risk management framework for information technology project. *International Journal of Information Management*, *32*(1), 50-65.

[4] Guo, F., Chang-Richards, Y., Wilkinson, S., & Li, T. C. (2014). Effects of project governance structures on the management of risks in major infrastructure projects: A comparative analysis. *International journal of project management*, *32*(5), 815-826.

[5] Marcelino-Sádaba, S., Pérez-Ezcurdia, A., Lazcano, A. M. E., & Villanueva, P. (2014). Project risk management methodology for small firms. *International journal of project management*, *32*(2), 327-340.

[6] Zwikael, O., & Ahn, M. (2011). The effectiveness of risk management: an analysis of project risk planning across industries and countries. *Risk Analysis: An International Journal*, *31*(1), 25-37.

[7] Chapman, R. J. (2011). *Simple tools and techniques for enterprise risk management*. John Wiley & Sons.

[8] Paape, L., & Speklé, R. F. (2012). The adoption and design of enterprise risk management practices: An empirical study.

European Accounting Review, *21*(3), 533-564.

[9] Rachmad, Y. E. (2012). *Enterprise Risk Management: Frameworks, Strategies, and Best Practices*. The United Nations and The Education Training Centre.

[10] Kardes, I., Ozturk, A., Cavusgil, S. T., & Cavusgil, E. (2013). Managing global megaprojects: Complexity and risk management. *International business review*, *22*(6), 905-917.

[11] Ahsan, K., Ho, M., & Khan, S. (2013). Recruiting project managers: A comparative analysis of competencies and recruitment signals from job advertisements. *Project management journal*, *44*(5), 36-54.

[12] Bromiley, P., McShane, M., Nair, A., & Rustambekov, E. (2015). Enterprise risk management: Review, critique, and research directions. *Long range planning*, *48*(4), 265-276.

[13] Chan, A. P., Yeung, J. F., Yu, C. C., Wang, S. Q., & Ke, Y. (2011). Empirical study of risk assessment and allocation of public-private partnership projects in China. *Journal of management in engineering*, *27*(3), 136-148.

[14] Nagpal, S., Khatri, S. K., & Kumar, A. (2015, May). Comparative study of ERP implementation strategies. In *2015 Long Island Systems, Applications and Technology* (pp. 1-9). IEEE.

[15] Nalluri, S. K., & Parasaram, V. K. B. (2015). Automating Software Builds with Jenkins: Design Patterns and Failure Handling. *International Journal of Technology, Management and Humanities*, 1(01), 16-33.

[16] Leka, S., Jain, A., Cox, T., & Kortum, E. (2011). The development of the European framework for psychosocial risk management: PRIMA-EF. *Journal of occupational health*, *53*(2), 137-143.