ISSN 2413-9610, E-ISSN 2663-2365 Journal homepage: https://devma.com.ua/en

DEVELOPMENT MANAGEMENT

UDC 004.042.2:658.5
DOI: 10.63341/devt/4.2025.48

Vol. 24, No. 4. 2025

Overview of risk management methodologies and standards in IT projects, programmes, and portfolioss

Mykyta Savchenko*
Master, Assistant
State University of Trade and Economics
02156, 19 Kyoto Str., Kyiv, Ukraine
https://orcid.org/0009-0004-9754-748X

Abstract. The study aimed to systematise existing risk management methodologies and identify theoretical provisions regarding their potential suitability for IT projects. To achieve this goal, a comparative analysis and theoretical assessment of the high-level characteristics of risk management methodologies in IT projects were used. The comparative analysis revealed the features of the most commonly used risk management methodologies: ISO 31000:2018 was characterised by a high level of versatility; Project Management Body of Knowledge (PMBoK) and Risk Management in Portfolios, Programs, and Projects: A Practice Guide had a high degree of detail; Projects IN Controlled Environments (PRINCE2) was formal in nature, while Enterprise Risk Management (COSO ERM) was conceptual; Factor Analysis of Information Risk (FAIR) and Factor Analysis of Information Risk Artificial Intelligence Risk (FAIR AIR) focused heavily on the use of quantitative risk assessment tools; and "NIST Special Publication 800-37. Revision 2. Risk Management Framework for Information Systems and Organisations: A System Life Cycle Approach for Security and Privacy", "NIST AI 100-1. Artificial Intelligence Risk Management Framework (AI RMF 1.0)" and "NIST AI 600-1. Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile" ensured risk management in projects based on the use of artificial intelligence. The results of comparative analysis and research into the practical application of individual methodologies can be used to select the optimal methodology in a specific context

Keywords: digital transformation; analysis; monitoring; control; software

INTRODUCTION

In modern conditions of digital transformation, effective risk management has become one of the key factors for the success of information technology (IT) projects, programmes and portfolios. The dynamic development of IT, the emergence of new architectural solutions, rapid software updates and high market competition create an environment of increased uncertainty. Effective risk management of IT projects is only possible if a wide range of external and internal project environment factors are addressed. It is necessary to emphasise the need to incorporate modern trends in the IT services market: the integration of artificial intelligence into the software production cycle, the ever-growing relevance of cybersecurity, cloud transformation as a strategic necessity, zero-trust architecture, DevOps and Infrastructure as Code, cost optimisation, low- and no-code platforms, distributed teams, and the transformation of stakeholder demand and expectations in the context of the popularisation of artificial intelligence.

There is no established taxonomy of IT project risks in the scientific field. In addition to the basic risks for project activities (such as failure to comply with project constraints, market and regulatory risks, human capital risks, etc.), IT projects are also characterised by specific industry risks. K. Nazarova *et al*. (2023) referred to risks related to IT infrastructure, personnel, loss or leakage of information, as well as social, legal, market and technological risks. The study addressed technological risks, which include risks of software code obsolescence, integration risks, and cybercrime risks. According to J.J. Selvakumar *et al*. (2024), risk management can improve the

Article's History: Received: 19.05.2025; Revised: 30.10.2025; Accepted: 23.12.2025; Published: 12.01.2026

Suggested Citation:
Savchenko, M. (2025). Overview of risk management methodologies and standards in IT projects, programmes, and portfolios. *Development Management*, 24(4), 48-56. DOI: 10.63341/devt/4.2025.48.

*Corresponding author

effectiveness of IT projects and initiatives. This conclusion was made based on the results of a structured survey of 261 IT professionals, emphasising the existence of a directly proportional relationship between risk identification and analysis and the probability of success of an IT initiative. The existence of such a relationship was also confirmed by R. Testorelli *et al*. (2024) in an investigation of the impact of risk management on the value of projects in various segments of the economy. Based on data from 116 relevant studies, the authors presented a theoretical model in which the use of risk management methodologies and tools increased the economic, environmental and social value of projects and programmes.

V.I. Ziuziun & D.O. Liashenko (2025) presented an integrated conceptual model of risk management for IT projects that create online platforms with high-value transactions, considering that traditional approaches, in particular ISO 31000:2018 (2018), PMBoK and MSF, do not fully meet the challenges of the digital environment, in particular fraud and cyber threats. The study emphasised that the modern information environment requires a rethinking of existing approaches and the introduction of new, contextually determined approaches. Thus, the effectiveness of risk management in projects, programmes and portfolios depends not only on specific risk management methodologies or standards, but also on the characteristics of the environment in which they are used. A similar opinion was presented by L. Mohylna & I. Vorobiov (2024), identifying and investigating the determining factors of risk management effectiveness in innovation and investment projects.

In addition to the need to align existing management methodologies and standards with company strategies, challenges lie in the lack of unified protocols for identifying and documenting risks. This obstacle to risk management was documented, for example, by W. Albasyouni *et al*. (2025), in a comparative analysis of individual companies from local and multinational corporations operating in the Middle East, Asia and Latin America. According to the observations, the key difference is that multinational corporations use standardised risk management protocols, while local companies often face difficulties in formalising these practices.

In the field of risk management methodologies and standards, it is also worth considering the sources of risk, which have been studied by A. Tak & S. Chahal (2024). According to these experts, existing sources of risk include dynamic resource allocation, management model sustainability, risk integration, and information quality. A. Tak & S. Chahal emphasised that analysis of the barriers to implementing existing methodologies and standards is key to effective risk management in projects and programmes. Despite the existence of individual studies comparing key risk management approaches and standards, there is a need for a more systematic and comprehensive review covering their conceptual foundations and practical applications. The study aimed to systematise international risk management methodologies and assess their relevance in the context of IT projects, programmes and portfolios. Achieving this goal involved conducting a comparative analysis and critical assessment of existing approaches to risk management in the segment under study.

MATERIALS AND METHODS

Key international standards and methodologies were used as primary materials, including ISO 31000:2018 (2018), A Guide to the Project Management Body of Knowledge PMBOK® Guide Seventh Edition (Project Management Institute, 2021) and PRINCE2 Project Management Foundation (Version 7) (PRINCE2, n.d.). Risk Management in Portfolios, Programs, and Projects: A Practice Guide (Project Management Institute, 2024) and NIST Special Publication 800-37. Revision 2 (National Institute of Standards and Technology, 2018) were also used. Alongside mentioned documents, the Factor Analysis of Information Risk (FAIR) (FAIR Institute, n.d.) and Committee of Sponsoring Organisations of the Treadway Commission Enterprise Risk Management (COSO ERM) (Committee of Sponsoring Organizations, n.d.) were also analysed. Alongside mentioned methods, the NIST AI 100-1. Artificial Intelligence Risk Management Framework (AI RMF 1.0) (National Institute of Standards and Technology, 2023), NIST AI 600-1. Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile (National Institute of Standards and Technology, 2024) and A FAIR artificial intelligence (AI) Cyber Risk Playbook (Copeland, 2024) were also analysed.

To achieve the research objectives and ensure the objectivity of the results obtained, a set of theoretical methods of scientific cognition, comparative analysis, and a review of the features of risk management in IT projects were used, which made it possible to comprehensively analyse the features of risk management in IT projects, programmes, and portfolios. The comparative analysis method was used to compare risk management methodologies and standards in terms of structure, process stages, level of detail, and practical application possibilities. Comparative analysis made it possible to identify common features, differences, advantages, and limitations in the context of modern IT projects, programmes, and portfolios. The comparison was made based on the following criteria: the fundamental idea that the methodology seeks to implement to create value; the level of detail, i.e. the depth of disclosure of the proposed processes and tools; degree of formalisation as the level of requirements for documenting and formalising processes; and adaptability, which consists in whether the methodology can be used for the modification of the proposed processes for a specific industry, organisation, portfolio, programme or project. The paper also examined the specifics of applying the selected methodologies in the context of risk management in IT projects. The practical aspect of using methodologies was explored in terms of their strengths and weaknesses in increasing project resilience in an environment of constant change.

RESULTS

International risk management standards

Risk management is a complex process with a high entry threshold, which often requires fruitful interaction between stakeholder groups, functional units of the organisation, corporate strategy and organisational culture. Given the complexity of this process, several international institutions aim to create universal methodologies that would accumulate the best and most relevant achievements in the scientific and practical spheres. This knowledge is systematised, tested for compliance with current conditions, and

transferred to managers in the form of ready-made models, processes, and tools. In other cases, risk management is an objective necessity due to the high cost of errors and regulatory restrictions, such as in data management, finance, and construction. In such cases, the creation of universal methodologies is part of the regulation of a given field of activity, and following the methodology becomes an obligation of the business entity. Risk management methodologies are often components of overall project management methodologies (as in the case of PRINCE2 and PMBoK), but for the most part, they are comprehensive and autonomous and can be studied separately.

The most popular risk management methodologies include ISO 31000:2018 (2018) (as well as related standards that cover individual elements of risk management in greater detail, such as IEC 31010:2019 (2019)), PMBoK (as well as the more detailed separately published methodology Risk Management in Portfolios, Programs, and Projects), PRINCE2, NIST Risk Management Framework (RMF), APM Project Risk Analysis and Management (PRAM), ISACA COBIT, FAIR, COSO ERM, and others.

ISO 31000:2018 (2018) is an international standard for risk management that sets out general principles, frameworks and processes for managing risks in any organisation. The methodology involves eight interrelated principles for creating and protecting project value: continuous improvement, use of the best available information, consideration of human and cultural values, consideration of the dynamic nature of the project, integration, structure and complexity, individualisation (customisation) and inclusiveness.

PMBoK is a framework of interrelated processes from the Project Management Institute (2021) (PMI) designed for project management; it considers project risk management as a separate set of processes, which includes identification, quantitative and qualitative risk assessment, response planning, and monitoring. In modern editions (7th edition and 8th edition), the approach has become more principled, adaptive, and focused on contextual selection of techniques. PMBoK is well-suited for medium and large projects where it is necessary to formalise risk management processes in the project lifecycle.

PRINCE2 (n.d.) is a project management methodology that originated in the United Kingdom and is widely used in government and corporate environments. In PRINCE2, risk is considered one of the key topics and, similar to ISO 31000:2018, provides for a cycle that includes risk identification, assessment, planning, implementation and communication. The methodology emphasises the appointment of risk owners, the use of a risk register and the inclusion of a risk strategy in the project's initial documents. A key feature of the methodology is its transparency, which is achieved through an emphasis on clear roles and responsibilities.

NIST Special Publication 800-37 is a methodology developed for managing information security risks. RMF consists of a sequential cycle of stages: organisation preparation, information system categorisation, security measure selection and implementation, assessment, authorisation, and continuous monitoring (National Institute of Standards and Technology, 2018). In contrast to the universal ISO 31000:2018, RMF is designed to ensure cyber resilience and compliance with government security standards in the field of IT. Its main advantage is the integration of risk management into the life cycle processes of IT systems.

FAIR is a universal risk management methodology that places a strong emphasis on the need to measure risks quantitatively, in financial terms, rather than solely in percentage or qualitative categories (FAIR Institute, n.d.). FAIR is based on two key concepts: loss event frequency and loss magnitude, which can be used for modelling the probability of risks occurring and their potential financial consequences. A distinctive feature of FAIR is its emphasis on a quantitative approach to risk assessment, which can be used for more informed budget allocation, risk prioritisation, and demonstration of the effectiveness of management measures. The methodology is used in the banking, financial, technology, and government sectors to build models of the economic effectiveness of cybersecurity.

The FAIR-AIR Approach Playbook is a variation of the FAIR methodology adapted to the conditions of artificial intelligence risk management (Copeland, 2024). This approach combines the principles of quantitative risk analysis with models for assessing specific risks associated with artificial intelligence (AI), such as algorithmic bias, opaque decisions, reputational damage, privacy violations, or failure to comply with ethical standards. The main difference between FAIR-AIR and FAIR is the object of assessment and the context of application: FAIR focuses primarily on information and cyber risks associated with technological systems; FAIR-AIR emphasises the risks arising from the implementation of artificial intelligence systems, where uncertainty often has not only technical but also socio-ethical dimensions. FAIR-AIR retains the quantitative basis of FAIR, but supplements it with an assessment of qualitative parameters such as user trust, ethical decision-making and algorithm transparency. This approach can be used for a comprehensive analysis of the risks of new technologies, ensuring a balance between business interests, security and social responsibility.

COSO ERM is a basic approach to corporate risk management (Committee of Sponsoring Organisations, n.d.). COSO defines risk management as a process implemented by the board of directors, management and other employees to identify potential events that could affect the organisation and manage risks within its risk appetite. The COSO model emphasises the integration of risk management with corporate strategy, culture and internal control systems. This approach can be used to create a unified structure in which risks are viewed not only as threats, but also as a source of strategic opportunities.

NIST AI 100-1 emphasised the management of risks associated with the development, implementation, and use of artificial intelligence systems (National Institute of Standards and Technology, 2023). This methodology focuses on transparency, fairness, accountability, and reliability of AI solutions. The AI RMF structure consists of four functions: building a risk management culture and integrating it with other business processes, mapping, measuring, and managing risks. The methodology provides recommendations for assessing potential ethical, technical, and social risks arising from working with machine learning algorithms and generative AI.

NIST AI 600-1 is a specialised profile that extends the AI RMF to generative artificial intelligence systems

(National Institute of Standards and Technology, 2024). This document details approaches to managing risks related to content creation, copyright, misinformation, and model bias. A substantial feature is the emphasis on data security, transparency of training samples, and human oversight mechanisms. A comparative analysis of risk management methodologies based on key parameters is presented in Table 1 below.

Table 1. Comparative analysis of key risk management methodologies in IT projects

Methodology/standard	Fundamental idea (value creation)	Level of detail	Level of formalisation	Adaptability
ISO 31000:2018 (2018)	Creation of a universal risk management system aimed at achieving the organisation's goals through the integration of risk management into all processes.	Medium – principles, frameworks and general processes are defined without excessive detail on tools.	Low – requires development of internal policies and procedures.	High – easily adaptable to most industries where risk management is not directly regulated.
PMBoK 6th edition (2017)	Formation of a structured risk management process within the project to control the impact of uncertainty on project objectives.	High – specific processes, inputs, outputs, tools and techniques are described.	Medium – clear requirements for documenting each risk management process.	High – easily adaptable to most industries where risk management is not directly regulated. The idea of adaptability ("fitting in") is embedded in the very foundation of the methodology.
PRINCE2 (n.d.)	Ensuring controlled project management through systematic risk management, roles and responsibilities.	High – specific processes, inputs, outputs, tools and techniques are described.	High – mandatory templates, roles, risk logs.	Medium – possible modifications within the approved management structure.
Risk Management in Portfolios, Programs, and Projects: A Practice Guide (2024)	Ensuring consistency in risk management across portfolio, programme and project levels to achieve strategic objectives.	High – the relationships between management levels are described in detail.	Medium – clear requirements for documenting each risk management process.	High – easily adaptable to most industries where risk management is not directly regulated.
NIST Special Publication 800-37 (National Institute of Standards and Technology, 2018)	Integration of information security risk management into the IT system lifecycle.	High – clear stages, control measures and audit requirements.	Very high – strict documentation and compliance with state standards.	Low – limited possibility of modification due to its regulated nature.
FAIR (n.d.)	Quantitative assessment of information risks in financial units for making economically sound decisions.	High – detailed models for calculating frequency and loss values are described.	Medium – requires data collection, but not strict formalism.	High – easily adaptable to the industry, system or type of risk.
COSO ERM (n.d.)	Integration of risk management into corporate strategy to create added value by balancing risks and opportunities.	Medium – principles, components and interrelationships are described, without specific techniques.	Medium – requires customisation of processes.	High – suitable for adaptation to most sectors and business scales. At the same time, in contrast to most other methodologies, it does not mention the principles and process of adaptation.
NIST AI 100-1 (National Institute of Standards and Technology, 2023)	Improving the reliability, fairness, transparency and accountability of artificial intelligence systems.	High – defined and detailed functions for building a risk management culture and integrating it with other business processes, mapping, measuring and managing risks.	Medium – clear requirements for documenting each risk management process.	Medium (within a specific subject area) – created as a flexible framework for different types of AI solutions.
NIST AI 600-1 (National Institute of Standards and Technology, 2024)	Managing risks associated with generative artificial intelligence: content, copyright, bias, and data security.	High – detailed risk categories for generative models.	High – requires strict documentation of processes and control measures.	Medium (within a specific subject area) – adapts within the field of generative AI.
FAIR-AIR (2024)	Quantitative assessment of artificial intelligence risks, including ethical, social and reputational aspects.	Medium – general processes are defined without excessive detail on tools.	Medium – requires basic documentation and qualitative justification.	Medium (within a specific subject area) – flexible methodology adapted to any AI systems and industries.

Source: compiled by the author based on Committee of Sponsoring Organisations (n.d.), FAIR Institute (n.d.), Project Management Institute (2021), J.B. Copeland (2024)

The comparative analysis showed that all the risk management methodologies considered have a common goal, which is to create a systematic approach to identifying, assessing and controlling risks to increase the resilience of organisations to uncertainty. They are all based on a process approach that includes the stages of risk identification, analysis, response and monitoring, ensuring continuous improvement of management practices. In addition, each methodology integrates risk management into the overall corporate or project management system and considers risk as a factor that can have both a negative and positive impact on the achievement of strategic goals.

At the same time, there are significant differences between the methodologies that determine their scope of application and the depth of procedure development. ISO 31000:2018 is distinguished by its high level of versatility and fundamental nature, as it emphasises not specific tools but general risk management principles, making it suitable for any organisation, including IT companies. PMBoK is characterised by a high degree of detail, while the PRINCE2 methodology is characterised by a high level of formalisation and a clear distribution of roles and responsibilities, which ensures transparency in risk management, especially in large IT projects or government structures. NIST Special Publication 800-37 has a strong technical focus and was developed primarily to ensure cybersecurity and information system risk management (National Institute of Standards and Technology, 2018). Its normative nature makes this approach particularly effective for the public and corporate sectors, where compliance with security standards is required.

COSO ERM, in turn, is a principle-based methodology that covers risk management at the strategic level of an organisation, creating a foundation for building a corporate risk management culture, but it needs to be adapted for practical use in the IT field. FAIR and FAIR-AIR are risk management methodologies that focus on quantitative risk assessment. FAIR can be used to express risks in financial terms, which is beneficial for the justification of investment decisions in business activities. FAIR-AIR is an extension of the basic FAIR model and is used to assess risks associated with artificial intelligence, including algorithmic, ethical and systemic risks, while maintaining a quantitative approach and enabling the economic value of the potential consequences of risks to be assessed. NIST AI 100-1 and NIST AI 600-1 are a separate category, representing methodologies for managing risks associated with the development and application of artificial intelligence systems (National Institute of Standards and Technology, 2023; 2024). While NIST AI 100-1 is a universal framework for building systematic risk management in AI, NIST AI 600-1 is its profile, specially adapted to generative artificial intelligence and aimed at managing the risks of transparency, bias, reliability and cybersecurity.

In the context of IT projects, the choice of risk management system should be based on the suitability of the methodology to the level of decision-making and the characteristics of the organisational environment. At the strategic level, it is possible to use ISO 31000:2018 and COSO ERM as tools that set out the general principles of integrated risk management, but the assumption of their increased effectiveness needs further verification. At the project level, any of the methodologies considered in the study can be effective, as their usefulness is determined by the specific conditions of the project implementation. NIST Special Publication 800-37 focuses on ensuring an adequate level of information security (National Institute of Standards and Technology, 2018). FAIR, along with the other methodologies mentioned, also supports quantitative risk assessment and uses common tools, such as Monte Carlo modelling; at the same time, its advantage lies in its systematic structure for the financial interpretation of risk indicators and the justification of the economic feasibility of management decisions. Finally, NIST AI 100-1, NIST AI 600-1 and FAIR-AIR are crucial in implementation of artificial intelligence technologies, as they cover the specifics of the subject area. Based on the characteristics of individual methodologies, it is proposed to consider an integrated approach that provides comprehensive risk management, from the strategic level to specific digital systems and algorithms, creating a reliable foundation for the sustainable development of IT organisations.

Assessment of high-level characteristics of risk management methodologies in IT projects

The practical application of modern risk management methodologies demonstrates that organisations can combine several approaches depending on their field of activity, IT environment structure, and level of regulatory complexity. In this context, ISO 31000:2018 serves as a universal framework for shaping organisational culture, establishing procedures for identifying, assessing and treating risks, and ensuring coordination between departments. The practical strength of this methodology lies in its ability to provide a universal assessment of existing risks and ensure strategic alignment, which is particularly useful for organisations with complex structures or a high degree of IT dependency. At the same time, the main limitation of ISO 31000:2018 is its generality: the methodology describes principles but does not contain detailed instructions for implementing processes. This forces organisations to either develop internal processes or turn to other, more organised and detailed methodologies.

An example of such a methodology is PMBoK, which provides structured risk management within projects. In practice, framework approaches are effectively applied where it is necessary to document risks, track their impact on deadlines, budget or quality, and coordinate interaction between different teams. The strength of this methodology is its systematic nature, which makes it possible to formalise processes and integrate risk management into the project life cycle. However, given the rise of agile development approaches, excessive formalisation can hinder teams working in highly dynamic environments. In such cases, it is advisable to adapt the application of PMBoK by reducing the amount of documentation and emphasising the role of regular communication and short risk review cycles.

Risk Management in Portfolios, Programs, and Projects delves deeper into the domain of uncertainty in project management and expands the scope to include programme and portfolio management (Project Management Institute, 2024). At the same time, the methodology focuses primarily not on scaling as simply the ability to cover a larger object, but on building a multi-level, holistic

corporate risk management system. The methodology reveals in detail the interrelationships between risk management levels, sets a clear framework of duties and responsibilities, and describes in detail the principles of effective interaction within and between levels. This ensures the complete versatility of the methodology in terms of its scope of application: it can be applied at the level of an individual project, programme or business unit, or it can be used as the basis for a corporate risk management system. The key challenge in implementing the methodology is the high requirements for corporate culture and maturity.

PRINCE2 (6th edition) can also be used to ensure the controllability of large projects, especially where strict change control and a clear accountability system are required. The practical advantage of the methodology is that it ensures transparency of decisions and predictability of results, which is relevant for IT initiatives in the public sector or in large transformation programmes. At the same time, the rigidity of PRINCE2 can be an issue in fast innovation cycles, where the focus of stakeholders shifts from controllability of the environment to speed and adaptability. In the field of information security, NIST Special Publication 800-37 is widely used in practice, enabling organisations to align their IT systems with industry and international standards (National Institute of Standards and Technology, 2018). The advantage of this methodology is its ability to ensure formalised compliance. However, the complexity and resource intensity of NIST Special Publication 800-37 can be an obstacle for organisations that do not have a developed information security function. To reduce the burden, it is recommended to apply NIST RMF selectively, focusing first on the most critical systems and then scaling the process to all IT assets.

Factor Analysis of Information Risk (FAIR) focuses on quantitative risk modelling and assessing the economic feasibility of response measures. Its key strength is its emphasis on financial consequences, which can be used for informed investment decisions. FAIR is widely used to model potential losses, assess the probability of incidents, and determine the optimal level of investment in response measures. At the same time, FAIR is dependent on quality data: the model operates at its highest efficiency when an organisation has sufficient historical and statistical data or can provide a correct assessment.

COSO ERM addressed the creation of a corporate risk management system, but in contrast to the PMI's framework, it focuses primarily on this level. This complicates the targeted implementation of the methodology locally at the level of individual projects. At the same time, COSO ERM can be cumbersome for organisations that do not have mature strategic management mechanisms. To overcome this, it is recommended to start with individual components of COSO ERM, such as the process of determining risk appetite or integrating risks into the budget cycle, gradually expanding the scope of application.

In the field of artificial intelligence, the latest frameworks NIST AI 100-1, NIST AI 600-1, and FAIR AIR provide practical mechanisms for controlling risks associated with incorrect predictions, generative system failures, or data leakage risks. Their competitive advantage is their specialisation in a specific, narrow field with in-depth disclosure of the specifics of working with its risks. The limitation is their relative novelty: organisations do not yet have established practices for effectively protecting artificial intelligence systems. It is recommended to start implementing the methodology with use-case profiles, which can be used to adapt requirements to specific AI systems.

During the theoretical comparison of the characteristics of the methodologies used, it was assumed that different approaches may have complementary strengths: ISO 31000:2018, due to its "lightness" and lack of formalisation, is well suited for forming general policies and principles of risk management at different levels of the organisation, PMBoK and PRINCE2 ensure operational discipline, PMI Risk Management in Portfolios, Programs and Projects provides tools for correct process scaling, NIST RMF ensures compliance with regulatory requirements and the highest standards, FAIR provides "light" and adaptive tools to improve the quality of management decisions based on quantitative risk assessment. COSO ERM builds flexible processes and principles for building a corporate risk management system, and the extension of some of these frameworks (NIST RMF, FAIR) can be adapted to the specific challenges of artificial intelligence systems. However, these conclusions are hypothetical and require empirical confirmation in different organisational contexts.

DISCUSSION

The key task of the study was to conduct a comparative analysis, which resulted in conclusions about the characteristics, strengths and weaknesses of individual risk management methodologies. The idea presented in the study regarding the need to compare and contextualise methodologies has been confirmed in previous studies, by B. Metin *et al*. (2024), arguing that objective risk assessment in the field requires analysis of information relating to business requirements, human factors and safety culture in the organisation. The ideas expressed by B. Metin *et al*. correlate with the theoretical comparison of the characteristics of methodologies presented in this study and the emphasis on the fact that each of them has both strengths and weaknesses in the context of risk management in IT projects. B. Teslim (2023) considered the idea that the effectiveness of risk identification and analysis is enhanced using artificial intelligence tools that facilitate rapid data collection and processing. Based on data obtained from 360 IT professionals, S. Kalogiannidis *et al*. (2024) concluded that AI-based data analysis and its integration into incident response planning improve risk assessment and support business continuity in an environment where enterprises face risks such as natural disasters, cyber-attacks, or economic fluctuations.

The presented study also considered the idea that the choice of risk management methodologies and standards largely depends on the context in which they are used. The idea of contextually determined choice of risk management methodologies was also confirmed in the study by I. Aswat & A. Carolin (2024). Experts noted that to improve the effectiveness of risk management, companies should further determine the needs and specifics of individual economic segments. This opinion partly correlates with the results of the study, but the difference lies in its different analytical focus. In contrast to I. Aswat & A. Carolin, who studied the accounting services sector, presented a study that analysed risk management methodologies in the IT segment.

A. Harju *et al*. (2024) analysed the risks arising for financial institutions when purchasing IT services, emphasising the specifics of the interaction between the financial sector and technology solution providers. This connection confirms the idea put forward in the work that the effectiveness of risk management methodologies and standards in the IT sphere largely depends on a detailed analysis of the context of their application and adaptation to the specifics of the project environment. A partial correspondence was also found between this work and the study by Y. Xu *et al*. (2024), which analysed the origins, connections and differences in the interpretation of risks in different disciplines and segments. The existence of such differences partly confirms the idea presented in this paper that context determines the assessment of risks and the choice of approaches to their minimisation. However, the correspondence is incomplete in the context of the relatively narrow scope of the presented study. Based on an analysis of the strengths and weaknesses of the most commonly used risk management methodologies, the paper considered the need for an integrated approach to risk management. This view has been confirmed in previous studies, for example, by D. Yuniarto & A.B.A. Rahman (2025). The thematic analysis of 61 scientific works presented by these researchers identified three groups of factors for the effective implementation and minimisation of risks in IT projects: support from the organisation's management, cross-functional cooperation, and risk-aware decision-making.

The results of the analysis indicate the feasibility of applying risk management methodologies in IT projects, particularly in the context of software development, to improve process control and timely identification of potential risks. After examining various risk minimisation and management strategies, O.T. Adebayo (2024) concluded that a proactive approach to threat management is effective. The study emphasised that risk management in the early stages of a project can ensure a timely response to potential threats. The general stages of risk management identified in the comparative analysis provide a basis for its implementation. The importance of early risk identification as an effective risk management strategy was also confirmed in the work of G. Kanyongo & N. Wadesango (2025). In contrast to the presented study, G. Kanyongo & N. Wadesango addressed cybersecurity risks. A high level of correspondence was also found between the presented study and the work of V.S. Balasubramaniam *et al*. (2023), in which the identification of risks in the early stages of the project life cycle was considered a substantial factor in the effectiveness of risk management in the field of IT. Overall, numerous similarities were identified between this study and previous works, suggesting the relevance of the chosen topic and the feasibility of further research. The contribution of this work to the existing academic discourse lies in its attempt to systematise and compare international methodologies and standards for risk management in the field of IT. A systematic analysis can be beneficial in managing new and existing risks in one of the most dynamic segments of the economy.

CONCLUSIONS

A comparative analysis revealed that methodologies differ in their level of detail. For example, ISO 31000:2018 has a high level of versatility, while PMBoK and Risk Management in Portfolios, Programs, and Projects: A Practice Guide are characterised by a higher degree of detail, focusing on risk management within the life cycle of projects, programmes, and portfolios. Key features of different risk management methodologies that may influence the choice of approach were also identified: PRINCE2 is characterised by a high level of formalisation, NIST RMF has a pronounced technical focus, COSO ERM is oriented towards building a risk management system in an organisation, while FAIR and FAIR-AIR provide structured quantitative risk assessment tools, which, however, are also used in many other methodologies.

The comparative analysis also revealed key features of NIST AI 100-1 and NIST AI 600-1, which are risk management methodologies for IT systems based on artificial intelligence. The limitations of the study are the theoretical scope and the need for further verification of the proposed strategies in the context of individual companies or projects. In future research, the use of empirical data collection tools, such as surveys, experiments, or statistical analysis, is recommended to support the above statements.

ACKNOWLEDGEMENTS

None.

FUNDING

None.

CONFLICT OF INTEREST

None.

REFERENCES

[1] Adebayo, O.T. (2024). Project risk management strategies: Best practices for identifying, assessing, and mitigating risks in project management. *IRE Journals*, 7(10), 371-381.

[2] Albasyouni, W., Kamara, J., & Heidrich, O. (2025). Key challenges and opportunities to improve risk assessments in the construction industry. *Buildings*, 15(11), article number 1832. doi: 10.3390/buildings15111832.

[3] Aswat, I., & Carolin, A. (2024). The role of information technology in risk management in the service sector (case study on accounting serviced firms in Pontianak). In *The 5th Asia-Pacific management research conference: "Adapting sustainability strategies in business and management"* (pp. 65-73). Pontianak: PPM School of Management. doi: 10.2478/9788367405850-007.

[4] Balasubramaniam, V.S., Mahadik, S., Khair, A., Goel, O., & Jain, A. (2023). Effective risk mitigation strategies in digital project management. *Innovative Research Thoughts*, 9(1), 538-567. doi: 10.36676/irt.v9.i1.1500.

[5] Committee of Sponsoring Organizations. (n.d.). *Guidance*. Retrieved from https://www.coso.org/guidance-erm.

[6] Copeland, J.B. (2024). *A FAIR artificial intelligence (AI) cyber risk playbook*. Retrieved from https://www.fairinstitute.org/blog/fair-artificial-intelligence-ai-cyber-risk-playbook.

[7] FAIR Institute. (n.d.). *What is FAIR?* Retrieved from https://www.fairinstitute.org/what-is-fair.

[8] Harju, A., Schaëfer, K., Hallikas, J., & Kähkönen, A.-K. (2024). The role of risk management practices in IT procurement: A case study from the financial services industry. *Journal of Purchasing and Supply Management*, 30(2), article number 100899. doi: 10.1016/j.pursup.2024.100899.
[9] IEC 31010:2019. (2019). *Risk management – risk assessment techniques*. Retrieved from https://www.iso.org/standard/72140.html.
[10] ISO 31000:2018. (2018). *Risk management – guidelines*. Retrieved from https://www.iso.org/standard/65694.html.
[11] Kalogiannidis, S., Kalfas, D., Papaevangelou, O., Giennarakis, G., & Chatzitheodoridis, F. (2024). The role of artificial intelligence technology in predictive risk assessment for business continuity: A case study of Greece. *Risks*, 12(2), article number 19. doi: 10.3390/risks12020019.
[12] Kanyongo, G., & Wadesango, N. (2025). Impact of cybersecurity on risk mitigation strategy by commercial banks in emerging markets: A legal perspective case study. *Corporate Law & Governance Review*, 7(1), 28-37. doi: 10.22495/clgrv7i1p3.
[13] Metin, B., Duran, S., Telli, E., Mutlutürk, M., & Wynn, M. (2024). IT risk management: Towards a system for enhancing objectivity in asset valuation that endangers a security culture. *Information*, 15(1), article number 55. doi: 10.3390/info15010055.
[14] Mohylna, L., & Vorobiov, I. (2024). Risk management of innovation and investment projects of an enterprise. *Economy and Society*, 66. doi: 10.32782/2524-0072/2024-66-130.
[15] National Institute of Standards and Technology. (2018). *NIST Special Publication 800-37. Revision 2. Risk management framework for information systems and organizations: A system life cycle approach for security and privacy*. Gaithersburg: National Institute of Standards and Technology. doi: 10.6028/NIST.SP.800-37r2.
[16] National Institute of Standards and Technology. (2023). *NIST AI 100-1. Artificial intelligence risk management framework (AI RMF 1.0)*. Gaithersburg: National Institute of Standards and Technology. doi: 10.6028/NIST.AI.100-1.
[17] National Institute of Standards and Technology. (2024). *NIST AI 600-1. Artificial intelligence risk management framework: Generative artificial intelligence profile*. Gaithersburg: National Institute of Standards and Technology. doi: 10.6028/NIST.AI.600-1.
[18] Nazarova, K., Parasii-Verhunenko, I., & Ostapets, A. (2023). Risk classification of IT industry companies. *Fruitful Knowledge*, 150(4), 120-137. doi: 10.31617/1.2023(150)08.
[19] PRINCE2. (n.d.). *PRINCE2® project management training*. Retrieved from https://www.prince2.com/eur/training/prince2?gad_source=1&gad_campaignid=22511484150&gbraid=0AAAABtHwdhs6aOdaoOdD17jgmG-DY-sU&gclid=Cj0KCQiArt_JBhCTARIsADQZaynyEP_2nY1VLht5VLZO1zIfy_CfcJybjkdcfkZll2ymv-It_OKPrpYaAlDgEALw_wcB.
[20] Project Management Institute. (2021). *A guide to the project management body of knowledge PMBoK® guide*. Newtown Square: Project Management Institute.
[21] Project Management Institute. (2024). *Risk management in portfolios, programs, and projects: A practice guide*. Newtown Square: Project Management Institute.
[22] Selvakumar, J.J., Suganya, G., Arthi, T.S., & Pachiyappan, S. (2024). Does risk management components influence on project success? Evidence from IT sector. *Journal of Project Management*, 9, 269-276. doi: 10.5267/j.jpm.2024.4.001.
[23] Tak, A., & Chahal, S. (2024). Risk management in agile AI/MI projects: Identifying and mitigating data and model risks. *Journal of Technology and Systems*, 6(3), 1-18. doi: 10.47941/jts.1824.
[24] Teslim, B. (2023). *Risk assessment in information security using AI: Utilizing predictive insights and threat modeling*. Retrieved from https://www.researchgate.net/publication/385746438_Risk_Assessment_in_Information_Security_Using_AI_Utilizing_Predictive_Insights_and_Threat_Modeling.
[25] Testorelli, R., Tiso, A., & Verbano, C. (2024). Value creation with project risk management: A holistic framework. *Sustainability*, 16(2), article number 753. doi: 10.3390/su16020753.
[26] Xu, Y., Reniers, G., & Yang, M. (2024). A multidisciplinary review into the evolution of risk concepts and their assessment methods. *Processes*, 12(11), article number 2449. doi: 10.3390/pr12112449.
[27] Yuniarto, D., & Rahman, A.B.A. (2025). Critical success factors for IT risk management in the digital transformation era: Insights from multiple case study. *Applied Information System and Management*, 8(1). doi: 10.15408/aism.v8i1.41090.
[28] Ziuziun, V.I., & Liashenko, D.O. (2025). Conceptual risk management model for the development of an online platform for high-value goods. *Collection of Scientific Works of NUK,* 1, 137-143. doi: 10.15589/znp2025.1(499).19.

Огляд методологій та стандартів управління ризиками в IT-проєктах, програмах та портфелях

Микита Савченко
Магістр, асистент
Державний торговельно-економічний університет
02156, вул. Кіото, 19, м. Київ, Україна
https://orcid.org/0009-0004-9754-748X

Анотація. Метою дослідження була систематизація наявних методологій управління ризиками та визначення теоретичних положень щодо їх потенційної придатності для IT-проєктів. Для досягнення поставленої мети був використаний метод компаративного аналізу та теоретичної оцінки високорівневих характеристик методологій управління ризиками в IT-проєктах. Компаративний аналіз дозволив виявити особливості найбільш часто уживаних методологій управління ризиками: ISO 31000:2018 характеризується високим рівнем універсальності; Project Management Body of Knowledge (PMBoK) та Risk Management in Portfolios, Programs, and Projects: A Practice Guide мають високий ступінь деталізації; Projects IN Controlled Environments (PRINCE2) носять формальний характер, а Enterprise Risk Management (COSO ERM) – концептуальний; Factor Analysis of Information Risk (FAIR) та Factor Analysis of Information Risk – Artificial Intelligence Risk (FAIR AIR) посилено фокусують увагу на використанні кількісних інструментів оцінювання ризиків; а «NIST Special Publication 800-37. Revision 2. Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy», «NIST AI 100-1. Artificial Intelligence Risk Management Framework (AI RMF 1.0)» та «NIST AI 600-1. Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile» забезпечують управління ризиками в проєктах, які базуються на використанні штучного інтелекту. Результати компаративного аналізу та дослідження особливостей практичного застосування окремих методологій можуть бути використані для обрання оптимальної методології в конкретному контексті

Ключові слова: цифрова трансформація; аналіз; моніторинг; контроль; програмне забезпечення