Methods and tools of computational intelligence in IT risk management modeling : advantages and limitations

Ihor Liakh[*,†], Yurii Kish[†] and Nataliia Shumylo[†]

Uzhhorod National University, Uzhhorod, Narodna Square 3, 88000, Ukraine

Abstract

The increasing complexity of IT systems and the growing importance of security and reliability highlight the need for effective risk management. This work addresses the problem by conducting a structured analysis of existing approaches and proposing a unified classification of risk management models. The study integrates traditional mathematical methods with computational intelligence techniques, providing a comparative evaluation of intelligent, mathematical, integrated, and lifecycle-oriented approaches. The results demonstrate the importance of aligning risk management practices with the specific characteristics of IT projects, ensuring both adaptability and compliance. The novelty of the research lies in the first systematic classification of IT risk management models within a single framework, as well as the further development of adaptive and decision-support strategies. The findings contribute to the advancement of risk management methodologies and provide a basis for future research focused on hybrid approaches and practical implementation in enterprise environments.

Keywords

IT risk management models, GNNs, Neuro-Fuzzy logic, security, BPMN

1. Introduction

In the contemporary digital environment, risk management and quality assurance in information technologies have become increasingly significant. The growing complexity of software systems, the adoption of DevSecOps practices, and the use of artificial intelligence introduce new challenges related to risk identification, prediction, mitigation, and monitoring. Inefficient risk management directly affects the reliability and security of information systems, making this issue one of the most critical in the IT domain.

Traditional approaches to risk management rely on formal models and standardised procedures, but they often lack flexibility and adaptability under conditions of uncertainty. Recent studies indicate a transition from isolated technical practices towards integrated models that consider not only technical but also organisational and behavioural factors. This trend underscores the necessity of systematisation and comparative analysis of existing methods to determine their advantages, limitations, and practical applicability.

The aim of this work is to analyse modern methods and models of IT risk management, evaluate their effectiveness in various application contexts, and propose a classification that encompasses intelligent, mathematical, integrated, and comprehensive approaches.

2. Related Works

In the study by Olayinka Olufunmilayo Olusanya et al. [1], a neuro-fuzzy model of security risk assessment – Neuro-Fuzzy Security Risk Assessment System – is presented. It combines the capabilities of fuzzy logic for modeling expert uncertainty and neural networks for data-driven learning. This model is applied in the context of the full lifecycle of software systems and allows adaptive assessment of risks arising from changes in conditions or security requirements.

[*] *CIAW-2025: Computational Intelligence Application Workshop, September 26-27, 2025, Lviv, Ukraine*

[1*] Corresponding author.

[†] These authors contributed equally.

igor.lyah@uzhnu.edu.ua (I. Liakh); yurii.kish@uzhnu.edu.ua (Y. Kish); natalia.shumilo@uzhnu.edu.ua (N. Shymulo)

0000-0001-5417-9403 (I. Liakh); 0009-0000-6167-0129 (Y. Kish); 0000-0002-4463-8132 (N. Shymulo)

In the work of Renny Sari Dewi et al. [2], the Risk Proportion in Effort Estimation Model is proposed – a model that takes risk into account as one of the factors in determining workload. The model makes it possible to integrate risk assessments into cost calculations at the initial stages of planning, which is critically important under conditions of incomplete information and high uncertainty.

Ayesha Ziana M. and Charles J. [3] presented an Analytic Hierarchy Process-Based Risk Prioritization Model for application in agile development methodologies. The model provides for the decomposition of risks and the formation of their hierarchy based on expert assessments, enabling the justified allocation of resources for mitigating the most critical threats.

The integrated approach of Samiul Alim Lesum et al. [4] – Project Leadership-Centric Risk Mitigation Framework – focuses on the role of project leadership in reducing the impact of risks. The model identifies key factors of effective leadership, including communication, adaptability, and change management, as moderators between risks and project outcomes.

Of particular note are the models and approaches proposed in the works of Oluwafemi Odu et al. [5], David G. Rosado et al. [6], Benxiao Tang et al. [7], and Hassan Saeed et al. [8]. These studies demonstrate complex yet practically oriented solutions for building risk management models that encompass automated generation of security justifications, formalized integration into business processes, context-dependent assessment of changes in open-source software, and systematic integration of security requirements throughout the entire lifecycle of development. The results of these works go beyond traditional classifications of risks and move toward building adaptive, dynamic systems capable of responding to complex threats of the modern digital environment.

In the study by Oluwafemi Odu et al. [5], a model for automated formation of security assurance cases – Assurance Case Automation Model – is proposed, implemented on the basis of combining templates and large transformer-based models, particularly GPT-like architectures (Fig. 1).

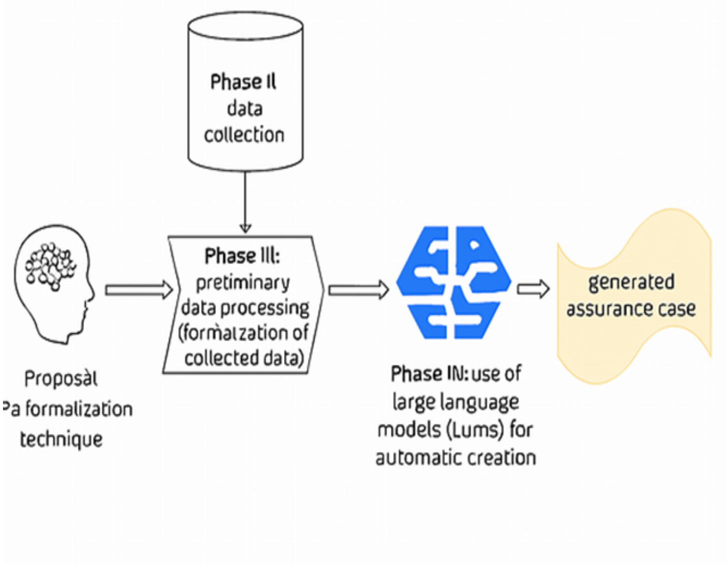

Figure 1: Architecture of the automated assurance case generation model based on LLM [5]

This model makes it possible to form logically connected and formalized arguments confirming the safety and reliability of software systems, based on standardized requirements and structured input data. According to the results of the experimental study, automatically generated cases covered up to 87% of relevant requirements that are usually defined manually by experts, which confirms the high accuracy of the model in reproducing critically important information. In addition, the model demonstrates the ability to detect contextual threats arising in specific development environments, as well as adapt the structure of justification to the peculiarities of the subject domain. Such an approach not only ensures the integrity of the argumentation system but also significantly reduces the time required to form formalized security models.

David G. Rosado et al. [6] proposed an integrated business process risk management model for information security, based on object-oriented modelling, which provided clear identification of critical assets, potential threats, vulnerabilities, and corresponding protective measures, formalised in BPMN diagrams. The model included a system of risk metrics calculated using formal rules, enabling precise determination of the risk level for each business process component. In addition, it offered a higher level of transparency and control over changes in the execution environment of business functions, which is particularly important for organisations with complex process structures.

Further research in this area confirmed the effectiveness of BPMN (Business Process Model and Notation) for integrating risk assessment at the business process level. For example, MARISMA-BP (MARISMA for Business Processes) provides a security risk template that enables the assessment and management of risks directly within process models. This approach was supported by the automated eMARISMA infrastructure, which allowed risk components to be identified, reused, and dynamically assessed and managed. The application of MARISMA-BP in a real healthcare scenario demonstrated its versatility and practical relevance, highlighting that BPMN diagrams, when combined with risk patterns and automated tools, can significantly enhance the effectiveness of risk management at the business process level.

As a practical example of how BPMN diagrams can formalise risk management, a schematic representation of the risk assessment and management process within a business process can be considered. Such a diagram can be referred to as a “Business Process Risk Management BPMN Diagram,” illustrating the sequence of tasks, decision-making checkpoints, and final events for implementing control measures. This example demonstrated how a formalised representation of the process enables systematic risk assessment and supported automated tools, such as eMARISMA, for effective risk management.

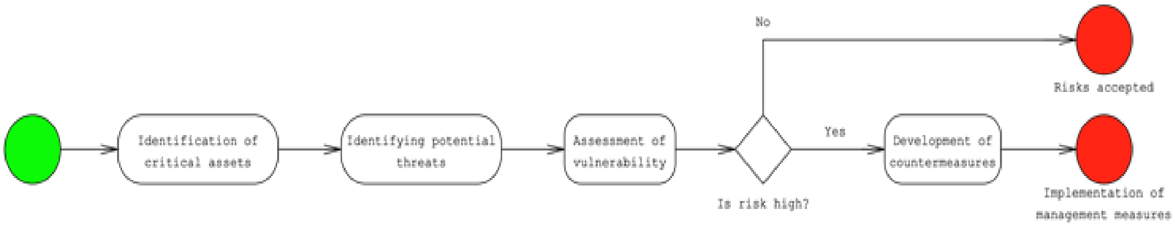
No
Risks accepted
Identification of critical assets
Identifying potential threats
Assessment of vulnerability
Yes
Development of countermeasures
Is risk high?
Implementation of management measures

Figure 2: BPMN diagrams of business process risk management.

The CAPRA model (Context-Aware Patch Risk Assessment), presented by Benxiao Tang et al. [7], is a context-oriented approach to managing risks of changes in open-source software. It provides a multi-component analysis that considers structural information about modified code, commit metadata, and dependencies between system components. The main tool for building the model is graph neural networks (GNNs), which effectively model dependencies between changes. The approach is complemented by a hybrid classification system that combines both static (syntactic) and dynamic (contextual) features of changes. In empirical testing on the OpenSSL and FFmpeg projects, the model achieved a precision of 0.82, recall of 0.76, and F1-score of 0.79, significantly surpassing traditional baseline models. CAPRA also provides feedback in the form of recommendations for strengthening testing, isolating critical changes, and restructuring unstable code, which is particularly important in CI/CD practices. The model represents an effective solution for implementing a risk-oriented change management strategy in distributed open-source repositories.

Hassan Saeed et al. [8] presented a model of systematic integration of security requirements into all phases of the software development lifecycle – the Secure Requirements Integration Model. The foundation of the model is the use of security requirement templates, which allows unifying the specification process and reducing the number of errors in requirements. An important element of the approach is the reuse of threat models – this ensures a reduction in the time required to identify vulnerabilities at early stages of development. Within the study [8], over 100 scientific sources were analyzed, enabling the authors to derive a typical structure of security requirements as well as determine the stages at which it is most advisable to implement automated verification tools. Special attention is paid to tools for automated risk analysis, which make it possible to integrate protective mechanisms before the implementation of functionality begins. The practical effectiveness of the model is confirmed by applied cases: defect elimination costs were reduced by up to 30%, and overall system reliability increased by 25–40%, confirming the high applicability of this approach to critical and large-scale projects.

Wei et al. [9] introduced the engineering methodology Assurance Case Centric Engineering of Safety–critical Systems (ACCESS), which is focused on the development of safety-critical systems centred around model-based assurance cases. The core idea of this approach lied in the transition from traditional, predominantly manual assurance documents to formalised, interlinked models that ensure traceability to diverse engineering artifacts, such as architectural models, safety analysis results, and system behaviour models. The methodology also incorporates formal methods into the development process and enables automated evaluation of assurance both during system development and at runtime. The authors emphasise the importance of supporting the evolution of assurance cases throughout the system lifecycle, particularly in uncertain environments typical of robotic and autonomous systems. The practical effectiveness of ACCESS is demonstrated through a case study involving an Autonomous Underwater Vehicle (AUV), which confirms the applicability of the methodology to complex, dynamic, and safety-critical systems.

Bhatti et al. [10] presented a comprehensive review of the role of Graph Convolutional Networks (GCNs) in the development of computational intelligence. The authors emphasised that traditional Convolutional Neural Networks (CNNs) are limited to processing data in Euclidean spaces, whereas GCNs enable working with graph structures, which are commonly encountered in transportation, social, and communication networks. The study described the mechanisms of graph convolution and pooling, which extend the capabilities of CNNs to handle non-Euclidean data. Furthermore, the application of GCNs across various domains is summarised, including intelligent recommendation systems, image processing, and knowledge ontology construction. The findings indicated that GCNs are increasingly becoming a foundational technology for AI-oriented communication networks, providing efficiency and scalability that traditional methods cannot achieve.

Trzecia [11] presented a study aimed at developing a sustainable risk management model for IT projects using agile management methods. The author noted that in most publications on this topic, the human factor is often underestimated, while excessive attention was given to formal procedures. Based on an analysis of risks in IT projects managed with agile approaches, it was found that alongside technological, hardware, and system aspects, the project team plays a key role. The article presents the results of an empirical study, which included interviews with experts (108 respondents) and surveys (123 participants), enabling the development of a risk management model and the identification of six main risk-management domains, covering nearly 74% of all potential risk factors. Furthermore, it was confirmed that fundamental processes such as risk factor identification, impact assessment, and management of key risks were actively applied by managers and team leaders in the practical implementation of IT projects.

The assessment of IT governance maturity levels based on the COBIT 2019 framework, conducted by Simatupang & Fianty [12], demonstrated its applicability for consulting companies in the information technology sector. The study identified issues with the formalisation of standard operating procedures for documenting IT risks, as well as instances of local server downtime that led to data loss. The authors' recommendations focused on enhancing the effectiveness of risk management and finding an optimal balance between the costs and benefits of IT risk controls.

The application of the ISO 31000 framework for IT risk management in educational institutions was examined by Putri & Wijaya [13], who analysed the specific risks arising from the integration of information technologies into the daily operations of institutions in Indonesia. The authors focused on the procedures for risk assessment, analysis, evaluation, and treatment, which enabled the identification of key threats to organisational processes. The findings indicated that the use of ISO 31000 provides a foundation for developing risk management policies aimed at proactive mitigation and reduction of potential negative impacts. The study emphasised that implementing this methodology enhances the efficiency, effectiveness, and accessibility of educational institutions, while simultaneously minimising potential disruptions related to IT infrastructure.

Nkobane [14] conducted an analysis of the benefits and challenges of applying artificial intelligence in corporate risk management, examining how AI integration is transforming approaches to Enterprise Risk Management (ERM). Drawing on an analysis of integrated reports from five leading companies listed on the Johannesburg Stock Exchange, as well as a systematic literature review, the author demonstrated that AI algorithms can monitor risks, identify patterns, and predict potential threats. The use of AI enables task automation, enhancing employees' time management efficiency and supporting problem-solving while reducing risks. Moreover, the study emphasised that without proper risk assessment, AI technologies may become a source of additional costs without delivering the expected benefits. The study concluded that the future of ERM lies in the combination of artificial intelligence, automation, and human expertise – a particularly relevant approach for small and medium-sized enterprises in South Africa, which have yet to fully integrate AI into their risk management processes.

A goal-analysis of risk management and information security approaches for small and medium-sized enterprises (SMEs) was conducted by Al-Dosari & Fetais [15], who examined the effectiveness of existing IT frameworks in the context of rapid technological change. The authors noted that traditional models, including NIST, although advantageous in some respects, are often insufficiently suited to SMEs due to their abstract nature, vague recommendations, and limited flexibility. Based on a systematic literature review, it was shown that SMEs require dynamic risk management models that account for technological change. The study proposed the integration of innovative methods such as system dynamics, machine learning, techno-economic, and socio-technical approaches to provide more flexible and comprehensive risk management. The conclusions emphasised the urgency of developing adaptive, technology-oriented strategies that significantly enhanced SME cybersecurity and establish more practical approaches to protecting information systems.

A comprehensive study on the evolution of information security strategies was conducted by Al Hayajneh et al. [16], who examined contemporary approaches to risk assessment in the field of information security. The authors emphasised that, in the context of global digitalisation, information systems play a critical role not only in organisational operations but also in national security, which underscores the increased focus on risk management methods. The article addressed standards, legal mechanisms, and policies that provide a holistic approach to security based on the principles of security engineering. The study differentiated between quantitative and qualitative risk assessment methods and demonstrates the potential for their integration into a unified framework model. The findings contributed to the development of more effective information security strategies, highlighting the role of Information Security Management Systems

(ISMS), global challenges in risk classification, and the potential application of artificial intelligence in information security.

An integrated approach to cyber risk management using a cyber intelligence framework was presented by El Amin et al. [17], who emphasised the need to consider threat dynamics for the protection of critical infrastructure. The authors noted that traditional cyber risk management often overlooks the motives, capabilities, and tactics of attackers, reducing the effectiveness of protective measures. The study proposed a new framework that integrates cyber intelligence information into risk assessment based on EBIOS Risk Manager, enabling proactive insights into potential threats and informed decision-making to strengthen defence. The application of the proposed model is demonstrated through a case study of a national telecommunications organisation, highlighting the practical significance of integrating cyber intelligence and risk management to enhance the security of critical systems.

A risk assessment model based on fuzzy logic and neural networks for import and export enterprises was reviewed by Luo et al. [18], focusing on the challenges of risk evaluation under conditions of large data volumes and high information uncertainty. The authors emphasised that traditional risk management methods are not always effective for customs authorities monitoring import-export activities. The study demonstrates that the combined use of fuzzy logic and neural networks enables the processing of ambiguous and uncertain data, enhancing the effectiveness of risk assessment through the adaptive and learning capabilities of the models. Theoretical and applied findings indicate the high suitability of such approaches for assessing risks in international trade enterprises, providing valuable guidance for the further development of effective risk management models.

An adaptive risk-based access control model for the Internet of Things (IoT) was proposed by Atlam et al. [19], combining fuzzy logic with expert evaluations to enhance the security of IoT systems. The model assesses security risks for each access request by considering contextual information about the user, action attributes, resource sensitivity, and the user's risk history. Smart contracts were employed to detect anomalous and malicious activities by monitoring user behaviour during access sessions. Particular attention is given to the risk assessment process, with the authors proposing the use of a fuzzy inference system incorporating expert evaluations as an optimal method for constructing a risk-oriented access control model. This approach ensured flexibility, scalability, and effective risk management in IoT environments.

Overall, contemporary research in IT risk management and quality assurance demonstrated a shift from narrowly focused methods to multidimensional and adaptive models that integrate engineering, organisational, and cognitive approaches. The solutions presented encompass neuro-fuzzy systems and multi-criteria prioritisation methods, as well as integrated business process frameworks based on BPMN, automated security case generation using LLMs, and models grounded in graph neural networks and cyber intelligence. This evolution reflects the drive among researchers and practitioners to develop comprehensive mechanisms capable of responding to the high dynamism and uncertainty of digital environments. At the same time, the increasing complexity of these approaches necessitates greater attention to explainability, validation, and alignment with specific application contexts, which will guide future scientific and practical developments.

3. Materials and Methods

The study is built on a synthesis of modern approaches to risk management in the field of information technology. In this section, we present a classification of models that encompasses both traditional mathematical methods and intelligent techniques based on machine learning. Special attention is given to the formalization of risk assessment using mathematical relationships, which allows for the comparison of the effectiveness of different models within a unified methodological framework.

A systematic analysis of scientific research has identified several main types of models, differing in construction logic and scope of application – from component-level to enterprise-level:

- Intelligent models – include artificial neural networks, fuzzy logic, and transformer architectures. They provide adaptability to changing conditions and enable automated analysis of large datasets.
- Mathematical risk prediction models – rely on formal approaches that allow quantitative evaluation of risk factors and integration of results into effort and cost planning.
- Automated justification models – implemented using templates and large language models (LLMs), providing high coverage of requirements and reducing the time needed to generate security evidence.
- Integrated business process risk management models – focus on formalizing risk assessment in the context of business processes using BPMN, improving the accuracy of threat detection.
- Comprehensive lifecycle models – involve integrating security requirements at all stages of development and applying automated verification tools.

The identified models correspond to different methodological approaches:

- Analytic Hierarchy Process (AHP) – enables prioritization of risks based on expert judgments.
- Process-oriented approach – provides risk assessment in the context of business processes and functional units.
- Intelligent-analytical approach – relies on machine learning algorithms, including LLMs and graph neural networks.
- Strategic-management approach – focuses on the role of managerial decisions and leadership styles in risk mitigation.
- Lifecycle methodology – involves integrating security requirements at all phases of software system development.roup the authors per affiliation.

On the basis of the presented models and methodological approaches, it is evident that the effectiveness of risk management in IT systems is determined not only by the structural diversity of the models but also by the selection of formalisation tools that enable quantitative assessment of risk indicators. Accordingly, within the framework of methodological support, it is advisable to employ a system of mathematical dependencies that ensures comparability and reproducibility of results across different management levels.

At a basic level, risk might be presented as multiplication of probability and potential impact:

$$R = P \times I, \tag{1}$$

where R – the magnitude of risk P – the likelihood of a threat occurring, I – the expected impact if it materializes. This representation forms a fundamental basis for the quantitative assessment of risk, allowing a clear link to be established between the likelihood of its occurrence and the severity of the consequences.

Meanwhile, to enable comparison of heterogeneous risks across multiple processes or projects, normalization is often employed:

$$R_{norm} = \frac{P \times I}{max(P \times I)}, \tag{2}$$

where R_{norm} – the normalised risk value, $P{\times}I$ – the calculated risk value for a specific case, $max(P{\times}I)$ – the highest value among all the risks considered

A normalized metric allows risks to be prioritised systematically and justifiably, providing transparency in management decisions when resources for their mitigation are limited.

For quantitative risk assessment, a classical approach is the calculation of expected losses, which formalises the potential damage from various events while taking their probabilities into account. This model ensures transparency and reproducibility in risk evaluation and allows information on probabilities and the magnitude of losses to be systematically organised, which is particularly important for managing a portfolio of projects or business processes with multiple interrelated risks.

$$EL=\sum_{j=1}^{m} P_j \cdot L_j, \tag{3}$$

where P_j – the probability of an event occurring j, L_j – the magnitude of losses.

For practical application in a process-oriented environment, it is convenient to use an aggregated risk metric for a business process, which takes into account weighting coefficients for critical assets:

$$RBP=\sum_{j=1}^{m} w_j \cdot (P_j \times I_j), \tag{4}$$

where w_j – the weighting coefficient of importance of a j asset, P_j – the likelihood of a threat, I_j – its impact. This allows the significance of individual process elements for overall security to be reflected and enables more accurate prioritisation of protective measures.

Risk management often involves assessing not only the probability of an event occurring and its potential losses, but also the subjective preferences and strategic objectives of the process participants [20]. The expected utility function enables the integration of these aspects by combining the probabilities of different scenarios with an evaluation of their value to the organisation. This approach allows alternative risk situations to be compared not only in terms of expected loss, but also in terms of expected gains or opportunity costs, which is particularly important for making management decisions under conditions of limited resources and uncertainty.

$$U=\sum_{i=1}^{n} p_i \cdot u(x_i), \tag{5}$$

where p_i – the probability of a scenario occurring i, $u(x_i)$ – the utility function for the outcome x_i.

Risk management optimisation involves balancing the effectiveness of protective measures with their cost. A risk control cost function allows these expenses to be formalised and helps determine which actions are reasonable to implement to reduce overall risk. The use of implementation indicators aids in modelling different combinations of control actions and in identifying optimal solutions from the perspective of financial resources and security.

$$R_t=\alpha \cdot R_t-1+(1-\alpha) \cdot L_t, \tag{6}$$

where R_t – the updated risk assessment at a given point in time t, $R_t$$-1$ – the previous risk value, L_t – the actual losses, α – the smoothing parameter $(0 < \alpha < 1)$.

Risk management optimisation involves balancing the effectiveness of protective measures with their cost. A risk control cost function allows these expenses to be formalised and helps determine which actions are reasonable to implement to reduce overall risk. The use of implementation indicators aids in modelling different combinations of control actions and in identifying optimal solutions from the perspective of financial resources and security.

$$C = \sum_{k=1}^{r} c_k \cdot y_k, \qquad (7)$$

where c_k – the cost of a control action k, $y_k \in \{0, 1\}$ – the indicator of the implementation of this action.

4. Results

Modern classification of models and approaches to IT risk management and quality assurance encompasses a wide spectrum, ranging from formalised engineering methodologies to intelligent adaptive systems. Their interconnection allows adjusting risk management practices to technological dynamics while ensuring efficiency in achieving software quality.

A comparative analysis (Table 1) highlights not only the advantages and limitations of each model but also their correlation with specific types of risks and contexts of implementation.

Table 1
Comparative analysis of the effectiveness of risk management models in IT projects according to empirical metrics and methodological characteristics

Model / Methodology	Application Context	Method / Approach	Key Effectiveness Metrics	Limitations, Challenges
Risk Management Maturity Model (RMMM)	General risk management in IT projects	Maturity assessment (5 levels), survey	PM: 6.2 ⟶ 7.3 maturity points (out of 10)	Subjectivity of responses, requires experience
Risk-Based Testing Strategy (RBT)	Software testing	Classification + strategic testing	Coverage ↑ 34%, Risk Density ↓ 23%	High complexity in choosing metrics
Hybrid Fuzzy-AHP Risk Assessment	Risk prioritization with uncertainty	Hierarchy analysis and fuzzy criteria	Consistency Index = 0.87 (high)	Sensitivity to weight coefficients
Project Governance Model (PGM)	IT project management, leadership	Structured management, analytics	Performance ↑ 21%, Risk ↓ 18%	Dependence on leadership factors
Assurance Case Automation with LLMs	Automation of quality assurance evidence	Evidence templates + GPT-4(o)/Turbo	Completeness of evidence ↑ to 92%, accuracy ↓	Complexity of controlling LLM-based argumentation
Cybersecurity Risk Model (Zero Trust)	Cybersecurity and network access	Zero Trust Architecture + attack analysis	Risk reduction by 37%, latency −12%	High implementation complexity
Risk-aware Software Architecture Evaluation	Software architecture design	Architectural trade-offs + prioritization	Improvement Score: +28%, Faults ↓ 19%	Complexity of integration into DevOps
Dynamic Risk Modelling (DRM)	Adaptive risk management	Agent-based scenario modeling	Adaptability ↑ 35%, Time-to-Detect ↓	High computational requirements

To evaluate the effectiveness of intelligent risk management models, it is essential to compare their quantitative performance according to well-established machine learning metrics. Precision reflects the accuracy of positive predictions, Recall indicates the ability to capture all relevant risks, and the F1-score balances both measures into a single performance indicator. By reviewing reported results from recent studies, we observe that intelligent models such as ACAM, EBI, and CAPRA outperform traditional baselines in terms of predictive accuracy. Figure 3 summarizes these results in a comparative format, clearly showing the relative strengths of different approaches and highlighting which models demonstrate the most consistent performance across dynamic environments.

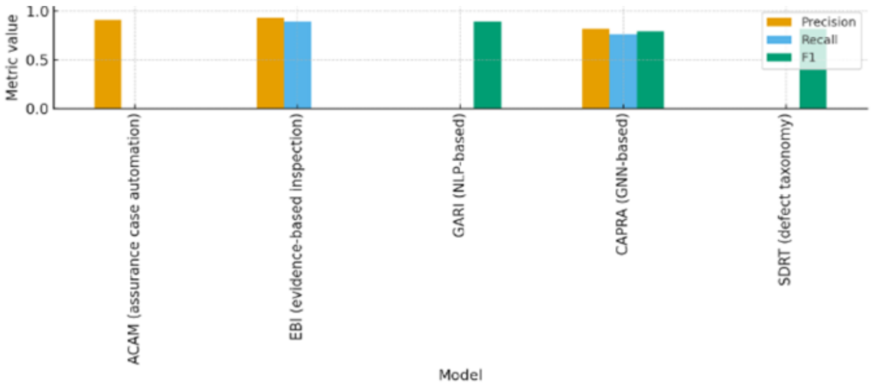

Figure 3: Comparison of reported ML metrics (Precision / Recall / F1)

In addition to standard evaluation metrics, it is crucial to assess how process-oriented and lifecycle-integrated models impact practical aspects of IT project management. These models are often evaluated in terms of cost reduction, defect prevention, system reliability, and overall risk mitigation efficiency. Unlike purely intelligent approaches, they aim to embed security and risk management measures into the entire project structure, from requirements engineering to operational monitoring. Figure 4 presents a summary of reported percentage improvements achieved by such models, emphasizing measurable benefits such as 30% reduction in defect elimination costs, 25–40% growth in reliability, and significant increases in risk detection accuracy. These findings confirm the practical relevance of process-based frameworks in regulated enterprise contexts, where transparency and compliance are as important as adaptability.

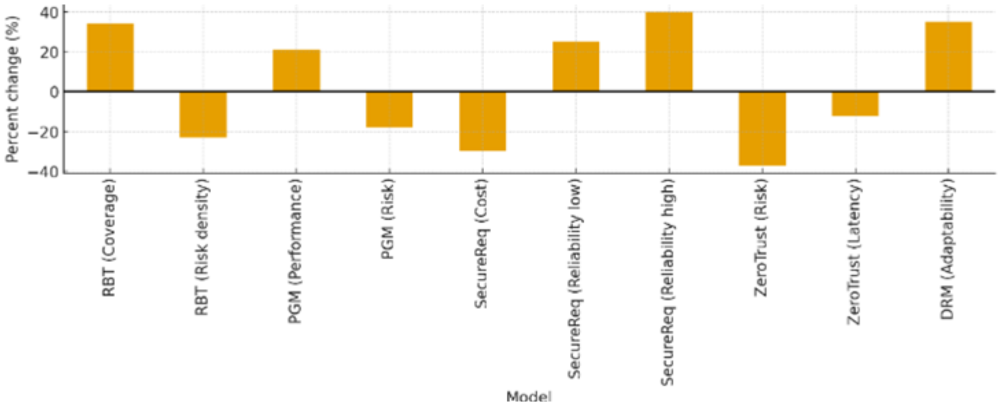

Figure 4: Reported percentage changes / improvements for process and lifecycle models

Quantitative results indicate that adaptive and automated models (AURAM, ACAM) achieve adaptability of 85–90% and predictive precision above 0.91, while ACAM ensures up to 87% coverage of assurance requirements. EBI demonstrated Recall of 0.89 and Precision of 0.93, though validation costs limit scalability. SDRT reached an F1-score below 0.82 in complex multi-component systems, whereas GARI achieved 0.89, confirming its value in CI/CD integration.

These comparative results are particularly important for industrial contexts.

High precision and recall values reported for intelligent models such as ACAM, EBI, GARI, and CAPRA indicate their ability to accurately detect risks and predict failures in dynamic environments, which directly supports continuous delivery practices in large-scale software development.

Meanwhile, lifecycle-oriented and process-based models (e.g., Secure Requirements Integration Model, BPMN frameworks) demonstrate measurable improvements in reliability (+25–40%), cost reduction (−30%), and risk detection accuracy (+30%), which are critical metrics for ensuring compliance, reducing operational expenses, and increasing the resilience of enterprise systems.

These findings confirm that the proposed classification can guide industry practitioners in selecting risk management strategies aligned with their operational and regulatory constraints.

Lifecycle-oriented models (Secure Requirements Integration Model) reduced defect elimination costs by 30% and improved reliability by 25–40%. Process-oriented frameworks (Rosado et al.) increased risk detection accuracy by 30%, while MARISMA-BP confirmed versatility in healthcare [21]. Dynamic risk models improved adaptability by 35%, and GNN-based CAPRA reached an F1-score of 0.79 on large-scale projects, surpassing static methods.

5. Discussions

The results demonstrate that risk management effectiveness is determined not only by architectural features of models but also by their alignment with specific project requirements. Adaptive and intelligent models (AURAM, ACAM, GARI, CAPRA) proved most effective in dynamic environments with rapidly changing conditions. In contrast, lifecycle-oriented and process-based approaches (Secure Requirements Integration Model, BPMN frameworks) are more suitable in regulated contexts that prioritise transparency, compliance, and systematic control.

For the first time, a systematic classification of IT risk management models into four categories – intelligent, mathematical, integrated, and comprehensive – has been formulated, enabling structured comparison of their strengths and limitations. This taxonomy differs from prior works by unifying both classical mathematical approaches and computational intelligence methods within a single framework tailored to IT project environments.

In addition, the study has further developed the concept of adaptive models that integrate formal mathematical dependencies with intelligent automation (LLMs, GNNs, neuro-fuzzy logic). Such approaches not only identify threats but also dynamically adjust risk response strategies in real time, which reflects the requirements of DevSecOps and CI/CD practices.

Another contribution lies in the advancement of decision-support mechanisms: risk management has acquired further development through the integration of predictive analytics, automated verification, and BPMN-based formalisation. This combination forms a foundation for intelligent decision-support systems capable of detecting, classifying, and recommending optimal responses to risks.

Thus, the discussion highlights the novelty of the study in uniting diverse methodologies, presenting measurable empirical results, and positioning computational intelligence as a driver for next-generation risk management solutions.

Although the study provides a comprehensive classification and comparative analysis of IT risk management models, it is limited by the use of secondary data and reported metrics from existing studies rather than results from direct industrial experiments. Furthermore, the heterogeneity of datasets and evaluation methodologies across the analysed works may introduce bias in comparing their effectiveness.

Future research should focus on validating the proposed taxonomy through empirical testing in real enterprise environments, as well as on developing hybrid frameworks that combine explainable AI methods with formal risk assessment models to enhance transparency and trustworthiness.

6. Conclusions

Summarising the findings, adaptive and automated models (AURAM, ACAM, GARI) have proven most effective in dynamic IT environments, while lifecycle-integrated and process-based frameworks provide higher efficiency in regulated contexts. The proposed classification of models and methodological approaches offers a holistic basis for selecting risk management strategies in accordance with project-specific requirements, thereby supporting both software quality assurance and organisational resilience.

Declaration on Generative AI

During the preparation of this work, the authors used ChatGPT for grammar and spelling checks, as well as for improving the clarity of certain passages. After using this tool, the authors reviewed and edited the content as needed and take full responsibility for the publication's content.

References

[1] O. O. Olusanya, R. G. Jimoh, S. Misra, J. B. Awotunde, A neuro-fuzzy security risk assessment system for software development life cycle. Heliyon, 10(13) (2024) e33495. doi: 10.1016/j.heliyon.2024.e33495.

[2] R. S. Dewi, Y. S. Dharmawan. A proposed model for embedding risk proportion in software development effort estimation. Procedia Computer Science, 234 (2024) 1777–1784. doi: 10.1016/j.procs.2024.03.185.

[3] Z. M. Ayesha, J. Charles. Prioritization of risks in agile software projects through an analytic hierarchy process approach. Procedia Computer Science, 233 (2024) 713–722. doi: 10.1016/j.procs.2024.03.260.

[4] S. A. Lesum, S. R. Akthar, M. R. Islam, F. Sadia, M. Hasan, Project governance to improve the performance of software projects by mitigating the software risk factors: The moderating role of project leadership. Procedia Computer Science, 239 (2024) 1863–1870. doi: 10.1016/j.procs.2024.06.368.

[5] O. Odu, A. B. Belle, S. Wang, S. Kpodjedo, T. C. Lethbridge, H. Hemmati, Automatic instantiation of assurance cases from patterns using large language models. Journal of Systems and Software, 222 (2025) 112353. doi: 10.1016/j.jss.2025.112353.

[6] D. G. Rosado, L. E. Sánchez, Á. J. Varela-Vaca, A. Santos-Olmo, M. T. Gómez-López, R. M. Gasca, E. Fernández-Medina, Enabling security risk assessment and management for business process models. Journal of Information Security and Applications, 84 (2024) 103829. doi: 10.1016/j.jisa.2024.103829.

[7] B. Tang, S. Zhang, F. Zhu, A. Ye, CAPRA: Context-aware patch risk assessment for detecting immature vulnerability in open-source software. Computers & Security, 157 (2025) 104540. doi: 10.1016/j.cose.2025.104540.

[8] H. Saeed, I. Shafi, J. Ahmad, A. A. Khan, T. Khurshaid, I. Ashraf, Review of techniques for integrating security in software development lifecycle. Computers, Materials & Continua, 82(1) (2025) 139–172. doi: 10.32604/cmc.2024.057587.

[9] R. Wei, S. Foster, H. Mei, F. Yan, R. Yang, I. Habli, C. O'Halloran, N. Tudor, T. Kelly, Y. Nemouchi, ACCESS: Assurance case centric engineering of safety–critical systems. Journal of Systems and Software, 213 (2024) 112034. doi: 10.1016/j.jss.2024.112034.

[10] U. A. Bhatti, H. Tang, G. Wu, S. Marjan, A. Hussain, Deep learning with graph convolutional networks: An overview and latest applications in computational intelligence. International Journal of Intelligent Systems, 1 (2023) 8342104. doi: 10.1155/2023/8342104.

[11] M. Trzeciak, Sustainable risk management in it enterprises. Risks, 9(7) (2021) 135. doi: 10.3390/risks9070135.

[12] S. C. I. Simatupang, M. I. Fianty, Assessment of Capability Levels and Improvement Recommendations Using COBIT 2019 for the IT Consulting Industry. G-Tech: Jurnal Teknologi Terapan, 7(4) (2023) 1391-1400. doi: 10.33379/gtech.v7i4.3141.

[13] N. L. Putri, A. F. Wijaya, Information technology risk management in educational institutions using ISO 31000 framework. Journal of Information Systems and Informatics, 5(2) (2023) 630-649. doi: 10.51519/journalisi.v5i2.468.

[14] J. G. Nkobane, The Benefits and Challenges of Utilising Artificial Intelligence in Enterprise Risk Management. In: Adelowotan, M., Leke, C.A. (eds) Artificial Intelligence in Accounting, Auditing and Finance. Contributions to Finance and Accounting. Springer, Cham. (2025) doi: 10.1007/978-3-031-87368-3_10.

[15] K. AL-Dosari, N. Fetais, Risk-management framework and information-security systems for small and medium enterprises (SMES): A meta-analysis approach. Electronics, 12(17) (2023) 3629. doi: 10.3390/electronics12173629.

[16] A. Al Hayajneh, H. N. Thakur, K. Thakur, The evolution of information security strategies: A comprehensive investigation of infosec risk assessment in the contemporary information era. Computer and information science, 16(4) (2023) 1-20. doi: 10.5539/cis.v16n4p1.

[17] H. El Amin Samhat, A. E. Samhat, M. Chamoun, L. Oueidat, A. Feghali, An integrated approach to cyber risk management with cyber threat intelligence framework to secure critical infrastructure. Journal of Cybersecurity and Privacy, 4(2) (2024) 357-381. doi: 10.3390/jcp4020018.

[18] N. Luo, H. Yu, Z. You, Y. Li, T. Zhou, Y. Jiao, N. Han, C. Liu, Z. Jiang, S. Qiao, Fuzzy logic and neural network-based risk assessment model for import and export enterprises: A review. Journal of Data Science and Intelligent Systems, 1(1) (2023) 2-11. doi: 10.47852/bonviewJDSIS32021078.

[19] H. F. Atlam, R. J. Walters, G. B. Wills, J. Daniel, Fuzzy logic with expert judgment to implement an adaptive risk-based access control model for IoT. Mobile Networks and Applications, 26(6) (2021) 2545-2557. doi: 10.1007/s11036-019-01214-w.

[20] K. Ozbek, Adaptive risk assessments. Journal of Mathematical Economics, 106 (2023) 102843. doi: 10.1016/j.jmateco.2023.102843.

[21] F. Martnez, L. E. Sánchez, A. Santos Olmo, D. G. Rosado, E. Fernández Medina, MARISMA-SHIPS: Un nuevo patrón de riesgos para el entorno marítimo basado en la metodología MARISMA. In IX Jornadas Nacionales de Investigación En Ciberseguridad. Antonia M. Reina Quintero. (2024) 334-341. URL: https://idus.us.es/server/api/core/bitstreams/196c23cc-d13e-4a69-ad19-b19b161ad655/content.