UDC 004.738.5:005.591 DOI: https://doi.org/10.64076/iedc250920.01

The impact of risk management on IT product quality: a comparative analysis

Ihor Liakh
Uzhhorod National University, Uzhhorod
https://orcid.org/0000-0001-5417-9403
Yurii Kish
Uzhhorod National University, Uzhhorod
https://orcid.org/0009-0000-6167-0129

Abstract. *This article explores the impact of risk management on the quality of IT products across diverse contexts, including cybersecurity, supply chains, and critical infrastructures. By analyzing empirical studies, it highlights how proactive, data-driven, and adaptive approaches improve functionality, reliability, performance, usability, and security, ensuring long-term resilience.*

Keywords: *risk management, IT product quality, cybersecurity, reliability, resilience.*

In the modern digital economy risk management has become a central component of IT governance, shaping how systems are designed, tested, deployed, and maintained. The integration of risk management into IT product development directly affects key quality indicators such as functionality, reliability, performance, usability, and security.

Risk management in IT has evolved from a narrowly technical practice into a multidimensional discipline encompassing organizational, psychological, and technical perspectives. Eling et al. [1] investigated the role of cognitive biases, particularly optimism bias, in decision-making processes related to cyber risk management. Their study, involving over 1,000 risk professionals from finance and IT sectors in Switzerland, Germany, and Austria, revealed that 69% underestimated the likelihood of cyber incidents. This underestimation led to reduced investments in critical protective measures, such as intrusion detection systems, thereby undermining both reliability and security.

Fotis et al. [2] examined the economic and operational impact of cyber incidents, using the Norsk Hydro ASA ransomware attack as a case study. Their findings demonstrated that proactive measures such as employee training, security audits, and threat detection technologies reduced successful attacks by 50%. The case further revealed that structured incident response strategies reduced recovery times by 35% and financial losses by 25%. These results underscore the value of embedding risk management into corporate governance structures to maintain product performance and usability during disruptions.

Risk management models applied to critical infrastructure, such as nuclear power plants, demonstrate how technical modeling contributes to IT product resilience. Son et al. [3] developed a quantitative cyber risk model based on fault tree analysis, showing that applying structured countermeasures reduced the conditional core damage probability of nuclear reactors by 45–52%.

Similarly, Dhungana et al. [4] emphasized the importance of addressing scientific uncertainty in risk communication, especially in crisis-response systems. Their interviews with 35 experts showed that 80% considered uncertainty an essential element of risk models, while 65% highlighted deficiencies in communicating uncertainty to end users. Incorporating adaptive models improved IT system functionality and reliability in uncertain environments.

The pharmaceutical supply chain represents another environment where risk management directly affects IT product quality. Ciceri et al. [5] identified 84 relevant risks and prioritized 15 using the analytic hierarchy process. Their results indicated that addressing supply shortages, regulatory compliance, and demand forecasting improved system reliability, functionality, and productivity. This evidence illustrates the broader applicability of structured risk management to IT systems supporting supply chain management.

Risk management also plays a vital role in robotic process automation (RPA). Schlegel et al. [6] evaluated risks in RPA projects using an “impact-uncontrollability” matrix. Their findings revealed that active risk management improved RPA system reliability and functionality, while failure to address risks in integration led to reduced usability and security. Quantitative results showed that well-controlled projects achieved significantly higher success rates than poorly managed ones, confirming the value of systematic risk assessment.

Network analysis has recently been applied to risk management in large-scale engineering projects. Casotti et al. [7] developed a network analysis-enhanced risk management framework (NAE-RM) for nuclear plant construction. Their results indicated that identifying 13 central risks improved the accuracy of risk assessment by 38% compared to traditional methods. By adapting this approach to IT projects, organizations can enhance reliability, performance, and decision-making transparency.

Huber et al. [8] investigated the integration of Balanced Scorecard (BSC) and Enterprise Risk Management (ERM). Their study found that embedding ERM into BSC reduced strategic deviations by 15–25% in subsidiaries and increased organizational adaptability by 30%. These findings demonstrate how aligning risk management with strategic control tools directly improves IT product quality, particularly in reliability and security.

In industrial contexts such as ship maintenance, Wang et al. [9] used multi-agent swarm modeling to optimize risk management. Their simulations reduced overall risk levels by 23.8% and shortened delays by 18.7%. Applied to IT systems, such approaches improve functionality and productivity by simulating scenarios and preemptively addressing vulnerabilities.

Basile et al. [10] explored automated risk management in software security under hostile execution environments (MATE context). Their methodology reduced successful attacks by 76% while maintaining acceptable performance overhead (7%). This balance ensured improved reliability, security, and functionality, demonstrating the potential of automated approaches for modern IT environments.

Blockchain-based risk management has also proven effective in supply chain security. Akhavantaheri et al. [11] found that blockchain integration reduced the likelihood of counterfeit electronic components by 49.6% and decreased risky supply nodes by 31.2%. These results highlight blockchain's ability to enhance IT system reliability, security, and transparency without negatively affecting usability.

Despite these advances, certain approaches demonstrate limited effectiveness. For example, excessive reliance on Earned Value Management (EVM) in project risk management often results in insufficient adaptability. Soliman et al. [12] reported that applying EVM in Kuwait's infrastructure projects revealed delays of up to 715 days and cost overruns of 16%. While EVM can provide early warning signals, its lack of flexibility reduces its impact on IT product quality, particularly in dynamic environments. Similarly, decision-making distorted by optimism bias remains a persistent barrier to effective risk management.

The comparative analysis reveals that the most effective risk management strategies share certain characteristics: they are proactive, data-driven, adaptive, and technologically integrated. Methods such as FTA modeling, network analysis, automated MATE defenses, and blockchain-enabled supply chains consistently deliver high improvements in IT product reliability and security. Meanwhile, organizational frameworks such as BSC-ERM integration and RPA-specific matrices support performance, usability, and long-term resilience. Conversely, isolated or rigid approaches–such as optimism-biased decisions or inflexible EVM applications–fail to provide sufficient quality assurance in fast-changing IT environments.

This analysis confirms the central role of risk management in determining IT product quality. By directly influencing functionality, reliability, performance, usability, and security, risk management transforms IT governance from a reactive process into a proactive safeguard of organizational resilience. Empirical results demonstrate quantifiable benefits: 50% fewer successful attacks, 35% faster recovery, 45–52% lower conditional damage probabilities, and up to 76% reduced attack success in hostile environments. Organizations that adopt integrated, technologically supported risk management frameworks are better positioned to ensure IT product quality, safeguard critical systems, and maintain long-term competitiveness in an increasingly risk-saturated digital environment.

References

1. Martin Eling, Kwangmin Jung, Optimism bias and its impact on cyber risk management decisions, Risk Sciences, Volume 1, 2025, 100001, ISSN 2950-6298, https://doi.org/10.1016/j.risk.2024.100001. (request date: 15.09.2025).

2. Friederikos Fotis, Economic Impact of Cyber Attacks and Effective Cyber Risk Management Strategies: A light literature review and case study analysis, Procedia Computer Science, Volume 251, 2024, Pages 471-478, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2024.11.135. (request date: 15.09.2025).

3. Kwang-Seop Son, Jae-Gu Song, Inhye Hahm, Jung-Woon Lee, Quantifying cyber risk: A model for evaluating safety impacts of cyber threats on NPPs, Nuclear Engineering and Technology, Volume 57, Issue 10, 2025, 103675, ISSN 1738-5733, https://doi.org/10.1016/j.net.2025.103675. (request date: 15.09.2025).

4. Annal Dhungana, Emma Hudson Doyle, Garry McDonald, Raj Prasanna, Navigating scientific modelling and uncertainty: Insights from hazard, risk, and impact scientists in disaster risk management (DRM), International Journal of Disaster Risk Reduction, Volume 118, 2025, 105260, ISSN 2212-4209, https://doi.org/10.1016/j.ijdrr.2025.105260. (request date: 15.09.2025).

5. Claudia Ciceri, Camilla Borsani, Michela Guida, Marco Farinelli, Federico Caniato, Impact pathways: navigating risks in the pharmaceutical supply chain – a multi-actor perspective, International Journal of Operations & Production Management, Volume 45, Issue 13, 2025, Pages 53-62, ISSN 0144-3577, https://doi.org/10.1108/IJOPM-06-2024-0458. (request date: 16.09.2025).

6. Dennis Schlegel, Oliver Fundanovic, Patrick Kraus, Rating Risks in Robotic Process Automation (RPA) Projects: An Expert Assessment Using an Impact-Uncontrollability Matrix, Procedia Computer Science, Volume 239, 2024, Pages 185-192, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2024.06.161. (request date: 16.09.2025).

7. André L.N. Casotti, Enrico Zio, Network analysis-enhanced project risk management for nuclear power plant construction, Reliability Engineering & System Safety, Volume 263, 2025, 111269, ISSN 0951-8320, https://doi.org/10.1016/j.ress.2025.111269. (request date: 16.09.2025).

8. Christian Huber, Kalle Kraus, Anita Meidell, Integrating the balanced scorecard and enterprise risk management: Exploring the dynamics between management control anchor practices and subsidiary practices, Management Accounting Research, Volume 66, 2025, 100924, ISSN 1044-5005, https://doi.org/10.1016/j.mar.2024.100924. (request date: 16.09.2025).

9. Kewen Wang, Peng Dong, Weibing Chen, Rui Ma, Longyu Cui, Research on risk management of ship maintenance projects based on multi agent swarm model simulation method, Heliyon, Volume 10, Issue 19, 2024, e38785, ISSN 2405-8440, https://doi.org/10.1016/j.heliyon.2024.e38785. (request date: 17.09.2025).

10. Cataldo Basile, Bjorn De Sutter, Daniele Canavese, Leonardo Regano, Bart Coppens, Design, implementation, and automation of a risk management approach for man-at-the-End software protection, Computers & Security, Volume 132, 2023, 103321, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2023.103321. (request date: 17.09.2025).

11. Hirbod Akhavantaheri, Peter Sandborn, Diganta Das, Using sociotechnical network modeling to analyze the impact of blockchain for supply chain on the risk of procuring counterfeit electronic parts, Advanced Engineering Informatics, Volume 65, Part B, 2025, 103272, ISSN 1474-0346, https://doi.org/10.1016/j.aei.2025.103272. (request date: 17.09.2025).

12. Ehab Soliman, Khaled A. Alrasheed, Saqer Alghanim, Eshrak Morsi, Integrating risk management and earned value framework to detect early warning signs – Case study, Journal of Engineering Research, 2024, ISSN 2307-1877, https://doi.org/10.1016/j.jer.2024.05.029. (request date: 17.09.2025).