# *Information System Failures: Causes and Preventive Strategies Through Systems Engineering Tools and Techniques*

Roshni Kothanur Papanna
( Systems Engineering )
Wrexham University, Wales

*Abstract*— **Despite advances in technology and systems engineering, information systems continue to fail due to a combination of organizational, technical, human, and environmental factors. This paper examines the main causes of these failures and highlights how tools such as requirements engineering, risk management, lifecycle models, and quality assurance can mitigate them. It also emphasizes the importance of stakeholder engagement, governance, change management, and continuous improvement. Evidence suggests that a disciplined, systemic application of systems engineering principles can significantly reduce failure risk and enhance the reliability and performance of information systems.**

## I. Introduction

Information systems are integral to supporting organizational operations, decision making and long-term strategic goals, becoming even more complex and interconnected as digital transformation accelerates access public and private sectors. However, despite their critical role, these systems oftem fail leading to financial loss, reduced productivity, security risks, and even system abandonment. Failures typically result from a mix of organizational, technical, human, and environmental factors, many of which are preventable with proper understanding and proactive management during system development, Systems engineering offers a streuctured approach to designing, analysing and managing complex systems throughout their lifrecycle, utilizing tools such as requirements engineering, system modelling, risk analysis, and quality assurance practices. By applying these techniques, organizations can identify potential failure points early on and address them before they escalate. Furthermore, the success or failure of an information system is not solely dependent on technical factors but also on functional alignment and effective collaboration. Adequate information technologies, along with skilled management and stakeholder engagement during the development and implementation phases are crucial for success. This paper explores the key factors contributing to information system failures and evaluates systems engineering practices that help mitigate risks, demonstrating that many failures can be avoided through a holistic, evidence-based approach to system development. Drawing on academic research and established practices, it emphasizes the importance of early analysis, disciplined process and continuous improvement in ensuring the reliability and performance of information systems.

## II. Causes that affect the implementation of an Information system

### *A. Defining the Project Incorrectly*

Before developing or implementing an information system, an organization must clearly establish its necessity and objectives. Failing to do so often leads to poorly defined projects and system failure. Without a clear purpose, accurate requirements, priorities, and success criteria cannot be set, which may result in a system delivered on time and within budget but failing to meet business needs.Many failures stem from incomplete, ambiguous, or constantly changing requirements, which create confusion, rework, delays, and cost overruns. Insufficient stakeholder involvement early in the project can also lead to misaligned systems that do not meet actual user needs or organizational processes.A well-defined project should include clear business objectives, functional and non-functional requirements, identified stakeholders, and measurable success indicators. Investing in early analysis and requirements engineering reduces uncertainty, improves communication, and increases the likelihood of delivering an effective and valuable information system.

### *B. Misaligned Technological Solutions*

A wide range of information technologies—software, hardware, and communication tools—support information systems, but selecting the right technology is critical to achieving organizational goals. Poor choices, including under- or overestimating tool complexity, can hinder adoption and lead to system failure. Rapid technological evolution means some tools become quickly obsolete, and expensive or advanced technologies do not always guarantee better outcomes. While Big Data technologies offer high-speed processing of large, diverse datasets at relatively low infrastructure costs, many organizations adopt them unnecessarily, often replicating existing processes. Implementation can also be costly due to consultancy and integration, resulting in benefits similar to those of existing systems.

### *C. Ineffective Use of External IT Consultancy*

Inappropriate IT consultancy can result in poor or inconsistent technology choices during system implementation. Many organisations rely on external consultancy firms to manage IT projects due to limited internal expertise or reluctance to hire additional staff for temporary initiatives. While IT consultants are intended to increase the likelihood of project success by providing specialised knowledge, failures often occur when they do not fully understand the organisation's functional and non-functional requirements during the analysis phase. This can lead to systems that do not adequately support business processes or user needs.

Additionally, consultancy firms may rely on traditional development cycles, which often involve long delivery times before tangible results are visible. This can cause frustration among stakeholders and may ultimately lead to project cancellation. Effective consultancy should instead focus on integrating technology using agile development methods and user-centred design principles, which emphasise flexibility, faster delivery, and alignment with end-user needs. When these approaches are applied, organisations are more likely to achieve successful system implementation and maximise the value of the chosen technology.

## III. Causes that affect the functionality of an Information system

### A. *Limited Managerial Commitment*

Management style plays a critical role in strategic initiatives, which often require organizational changes when adopting new processes or information systems. Resistance to change is inevitable, but if senior management does not lead by example, lower-level employees are unlikely to embrace the system. Active use and trust in the system by top management reinforce its credibility and encourage organization-wide adoption.

### B. *Absence of Effective Performance Indicators*

Performance indicators measure and monitor progress toward strategic objectives, providing insights to identify deviations and take corrective actions. Common types include fulfillment, evaluation, efficiency, effectiveness, and management indicators. These metrics support process improvements, product development, and informed decision-making, enhancing overall organizational performance.

### C. *Resistance to Organizational Culture Change*

Organizational culture—the shared values and practices among employees—affects the adoption of information systems. Companies reliant on manual processes may resist new systems, even if they improve efficiency. Promoting a culture that embraces technology and encourages openness to change is essential for successful implementation and effective use of information systems.

## IV. Project Failure Factors and Inherent Complexity

Project failures often result from a combination of inadequate planning and inherent complexity, particularly in IT initiatives. Two types of projects are common: routine projects with well-defined scopes and few unknowns, which generally fail only if technical expertise is lacking, and complex projects with unclear scopes, many unknowns, and high uncertainty, where difficulties can arise early, even before client approval. Planning deficiencies, especially in defining and controlling scope, are major causes of failure. Complexity persists even with optimal methodologies, driven by project volatility, uncertainty, and structural alignment with management approaches. Additionally, external organizations often lack understanding of development processes, limitations, and maintenance requirements, further increasing failure risk.

## V. Tools for failure analysis

Failure Mode and Effects Analysis (FMEA) is a systematic method for identifying how a procedure, product, or system might fail to meet its intended performance. It analyzes potential failure modes under various conditions, often using mathematical models, and is typically applied before product release to evaluate robustness and assess impacts on safety, reliability, and effectiveness.

FMEA can be performed using bottom-up or top-down approaches. The bottom-up method, Failure Mode, Effects, and Criticality Analysis (FMECA), starts at the component level and progresses to the system, and is repeated whenever design changes occur. The top-down method, Fault Tree Analysis (FTA), begins with an undesirable event and traces its root causes through logical relationships, supporting problem-solving and risk management.

## VI. Key considerations for improving information systems

### A. *Governance and Project Management*

Governance shapes behavior both indirectly, through supervisory structures, and directly, through organizational forces. While it operates within legal and contextual frameworks, it does not dictate individual actions. In projects, governance functions at multiple levels, including programs and portfolios, providing the framework for initiating, executing, and reporting projects. Project governance influences how project management is applied, affecting decisions on project process mechanisms (PPMs) and their impact on project success. Governance models can be top-down, emphasizing shareholder outcomes, or bottom-up, focusing on process control and extending project management methodologies.

### B. *Risk Management in Projects*

Risk management in information systems (IS) development is a crucial part of overall project management and can significantly affect outcomes. It consists of two main components:

- **Risk evaluation**
- **Risk control**.

Risk evaluation involves identifying potential risks, analyzing them, and prioritizing them based on likelihood and impact, typically rated as low, medium, high, or very high. Once risks are prioritized, risk control focuses on developing mitigation plans, implementing them, and monitoring progress to minimize negative consequences. The primary goal of risk management is to reduce the adverse effects of risks on the project.

### C. *Principles of Security*

This section provides a brief introduction to key concepts in the software security domain. Understanding these principles is fundamental for discussing and implementing application security effectively.

- **Security by Design**
  Security should not be an afterthought or a mere add-on in system development. From the outset, relevant security requirements must be identified and integrated into the overall process and system design. Begin by establishing principles and policies as a foundation, and then incorporate security throughout the development lifecycle.

- **Fail Safe**
  This principle ensures that confidentiality, integrity, and availability are maintained when an error or fault occurs. Such conditions may result from attacks or from design or implementation failures. In all cases, the system should default to a secure state rather than an unsafe one.

- **Security by Default**
  Secure-by-default configurations are the most secure settings possible, even if they are not the most user-friendly. Settings should be determined through careful risk analysis and usability testing to balance security with practicality.

- **Secure the Weakest Link**
  The overall resilience of software depends heavily on the protection of its weakest components, whether code, services, or interfaces. Identifying and addressing the most vulnerable components first, until an acceptable level of risk is achieved, is considered best practice in security

## VII. Discussion

Information system failures rarely stem from a single technical flaw; they typically result from the interaction of organizational, human, and process-related weaknesses. Deficiencies in stakeholder engagement, governance, requirements definition, and change management often exacerbate technical challenges, increasing the likelihood of failure.

Systems engineering tools and techniques help address these issues. Requirements engineering improves clarity and alignment with stakeholder expectations, while risk management and modeling enable early detection and correction of potential failures. Governance and change management promote accountability, user acceptance, and organizational readiness, all critical for successful system adoption.

Overall, adopting a holistic, life-cycle-based approach that integrates technical, organizational, and human considerations allows organizations to better manage complexity, reduce failures, and enhance long-term system performance.

## VIII. Conclusion

Information system failures remain a significant challenge due to the complexity of systems and the interaction of technical, organizational, and human factors. These failures often stem from weaknesses in requirements definition, stakeholder engagement, governance, risk management, and change management.

Applying systems engineering tools—such as life-cycle models, requirements engineering, risk analysis, and verification processes—can mitigate many of these risks. Strong governance, stakeholder involvement, security by design, and continuous improvement are also critical for success. Adopting a holistic, evidence-based approach enables organizations to manage complexity, anticipate risks, and enhance system performance. Ultimately, reducing failures requires not only technical solutions but also organizational commitment, structured processes, and continuous learning throughout the system life cycle.

## References

[1] UK Government, "Principles of Secure by Design," [Online]. Available: https://www.security.gov.uk/policy-and-guidance/secure-by-design/principles/. [Accessed: 15-Dec-2025].

[2] K. Lyytinen and D. Robey, "Learning from Information Systems failures by using narrative and antenarrative methods," *ResearchGate*, 2015. [Online]. Available: https://www.researchgate.net/publication/275400081_Learning_from_Information_Systems_failures_by_using_narrative_and_antenarrative_methods. [Accessed: 15-Dec-2025].

[3] OWASP, "Security Principles," [Online]. Available: https://devguide.owasp.org/en/02-foundations/03-security-principles/. [Accessed: 15-Dec-2025].

[4] M. Radosavljević and M. Stojanović, "Information System Failures: Causes and Lessons," *Management Information Systems*, vol. 4, no. 1, 2009. [Online]. Available: https://www.ef.uns.ac.rs/mis/archive-pdf/2009%20-%20No1/MIS2009_1_3.pdf. [Accessed: 15-Dec-2025].

[5] A. Müller and B. Turner, "The Relationship between Project Governance and Project Success," *ResearchGate*, 2016. [Online]. Available: https://www.researchgate.net/publication/296703744_The_Relationship_between_Project_Governance_and_Project_Success. [Accessed: 15-Dec-2025].

[6] J. Ives and S. Olson, "The Role of User Participation in Information Systems Development: Implications from a Meta-Analysis," *ResearchGate*, 2004. [Online]. Available: https://www.researchgate.net/publication/220591875_The_Role_of_User_Participation_in_Information_Systems_Development_Implications_from_a_Meta-Analysis. [Accessed: 15-Dec-2025].

[7] C. Bjørn-Andersen, "Towards a stakeholder analysis of information systems development project abandonment," *ResearchGate*, 2005. [Online]. Available: https://www.researchgate.net/publication/221409507_Towards_a_stakeholder_analysis_of_information_systems_development_project_abandonment. [Accessed: 15-Dec-2025].

[8] S. Alharbi, "Causes of IT Project Failures," *Journal of Information Systems Education and Management*, [Online]. Available: https://www.jisem-journal.com/download/YIXFK3LI.pdf?utm_source. [Accessed: 15-Dec-2025].

[9] S. Salmerón, "Early Warning Signs of IT Project Failure," *IACIS*, 2024. [Online]. Available: https://www.iacis.org/iis/2024/3_iis_2024_185-199.pdf?utm_source. [Accessed: 15-Dec-2025].

[10] L. Rosen, "Early Warning Signs of IT Project Failure," [Online]. Available: https://csbweb01.uncw.edu/people/rosenl/classes/ops100/early%20warning%20signs%20of%20it%20project%20failure.pdf?utm_source. [Accessed: 15-Dec-2025].

[11] J. Mahdi, "Information Systems Project Risk Factors," *Old Dominion University Digital Commons*, [Online]. Available: https://digitalcommons.odu.edu/cgi/viewcontent.cgi?article=1019&context=emse_fac_pubs&utm_source. [Accessed: 15-Dec-2025].

[12] S. Alhassan et al., "Causes of Failure in the Implementation and Functioning of Information Systems," *The Science and Information (SAI) Conference*, vol. 11, no. 6, 2020. [Online]. Available: https://thesai.org/Downloads/Volume11No6/Paper_18-Causes_of_Failure_in_the_Implementation_and_Functioning.pdf?utm_source. [Accessed: 15-Dec-2025].

[13] K. Adeyemi, "An Investigation of Information Systems Project Failure and Its Implication on Organisations," *Academia.edu*, 2022. [Online]. Available: https://www.academia.edu/81896869/An_investigation_of_information_systems_project_failure_and_its_implication_on_organisations?utm_source. [Accessed: 15-Dec-2025].