

Technology Risk Management: Strengthening Organizational Resilience in a Digital Environment

Zamil Alshammari

DOI: <https://doi.org/10.5281/zenodo.23297114>

Published Date: 11-October-2026

Abstract: Technology has become an essential part of modern organizations, supporting communication, financial activities, customer services, operations, data management and decision-making. At the same time, greater dependence on technology has created new risks. Cyberattacks, system failures, data loss, technology obsolescence, third-party service failures and human error can interrupt business activities and cause significant financial and operational consequences. Technology risk management is therefore becoming an important part of organizational risk management. This article examines the role of technology risk management in reducing operational disruption and strengthening organizational resilience. It discusses major categories of technology risk and considers how organizations can identify, assess, treat and monitor these risks. Particular attention is given to cybersecurity, data protection, cloud computing, third-party technology providers, human factors and emerging technologies. The article argues that technology risk management should not be viewed as the responsibility of the IT department alone. Effective management requires cooperation between senior management, technology specialists, risk professionals and employees across the organization. The article also highlights the importance of continuous monitoring, employee awareness, testing and organizational learning. A proactive and integrated approach to technology risk can help organizations reduce vulnerabilities while improving their ability to respond to unexpected events.

Keywords: technology risk management, modern organizations, supporting communication, financial activities, customer services, organizational learning.

1. INTRODUCTION

Technology has changed the way organizations operate. Many activities that were previously performed manually are now supported by digital systems. Organizations use technology to store information, communicate with customers, process payments, manage employees, coordinate supply chains and make decisions. This dependence can provide major benefits, including greater efficiency, faster communication and improved access to information.

However, dependence on technology also creates risk. A failure in an important information system can affect an entire organization. A cyberattack can prevent access to business information, expose confidential data or interrupt customer services. A failure at a technology supplier can also affect an organization even when its own internal systems are operating normally.

The increasing use of cloud services, artificial intelligence, mobile technologies and interconnected systems has made the technology risk environment more complicated. Organizations therefore need to understand technology risk as part of their wider business risk rather than treating it as a purely technical issue.

Technology risk management involves identifying technology-related threats, assessing their potential consequences, selecting appropriate controls and continuously monitoring changes in the risk environment. The objective is not necessarily to eliminate every technology risk. Instead, organizations need to understand which risks are most significant and determine how they can be reduced to an acceptable level.

This article examines the importance of technology risk management and its contribution to organizational resilience. It considers the main sources of technology risk and discusses how organizations can develop a more integrated approach to managing them.

2. UNDERSTANDING TECHNOLOGY RISK

Technology risk can arise from failures, weaknesses or inappropriate use of technology. It can be internal or external and may result from technical, human or organizational factors.

One common example is **system failure**. Hardware breakdowns, software errors, network problems and power interruptions can make important systems unavailable. The effect of a failure depends on the organization's dependence on the affected system. A short interruption in a non-critical application may have little impact, while the failure of a payment, production or customer-management system could significantly disrupt operations.

Data risk is another major concern. Organizations hold increasing amounts of personal, financial and operational information. Loss, corruption, unauthorized access or inappropriate disclosure of this information can result in financial and reputational consequences.

Cybersecurity risk has become particularly important. Organizations face threats including ransomware, phishing, malware, denial-of-service attacks and unauthorized access. Cyber incidents can affect the confidentiality, integrity and availability of information.

Technology risk can also originate outside the organization. Organizations increasingly rely on cloud providers, software suppliers, payment providers and other technology partners. This creates **third-party technology risk**, where a problem involving an external provider can affect the organization's own operations.

The rapid pace of technological change creates another challenge. A system that is considered secure today may become outdated as new vulnerabilities and threats emerge. Technology risk management therefore needs to be continuous rather than based on a single assessment.

3. TECHNOLOGY RISK AND ORGANIZATIONAL RESILIENCE

Technology risk management has a direct relationship with organizational resilience. Resilience refers to the ability of an organization to withstand disruption, continue important activities, recover from difficulties and adapt to changing conditions.

Duchek (2020) describes organizational resilience as a capability involving anticipation, coping and adaptation. This perspective is useful for technology risk because organizations need to anticipate possible technology failures before they happen rather than simply responding after an incident.

For example, an organization can anticipate the risk of data loss by maintaining backups and testing recovery procedures. It can prepare for cyberattacks by implementing security controls and training employees. It can reduce dependence on one technology supplier by developing alternative arrangements.

These measures can reduce the impact of disruption. More importantly, they can help organizations recover more quickly when preventive measures are unsuccessful.

Technology risk management should therefore be considered part of resilience planning. An organization that understands its technology dependencies is better positioned to determine which systems are critical and what would happen if those systems became unavailable.

4. CYBERSECURITY AS A TECHNOLOGY RISK

Cybersecurity represents one of the most significant areas of technology risk.

The growth of digital transformation has expanded the number of systems and devices connected to organizational networks. Saeed et al. (2023) identify cybersecurity as an important challenge associated with digital transformation, particularly as organizations adopt technologies such as cloud computing, artificial intelligence and big-data systems.

Cybersecurity risk is not limited to technical vulnerabilities. Employees can also create risk through weak passwords, phishing responses, inappropriate sharing of information or failure to follow security procedures.

This means that cybersecurity requires both technical and organizational controls. Firewalls, encryption, authentication, monitoring and access controls can reduce technical vulnerabilities. However, these measures need to be supported by employee training, clear policies and management oversight.

Ransomware provides an example of why cybersecurity and continuity need to be connected. Preventing an attack is important, but organizations should also consider what happens if an attacker successfully compromises their systems. Backup arrangements, incident-response procedures and recovery plans can determine how quickly essential activities can resume.

5. DATA PROTECTION AND INFORMATION RISK

Data is one of the most valuable resources in many organizations. It supports decision-making, customer relationships, financial management and operational processes.

Technology risk management should therefore consider the entire information lifecycle. This includes how data is collected, stored, accessed, transferred, backed up and eventually removed.

Organizations should identify particularly sensitive or critical information and determine what could happen if it were lost or disclosed. Access should be provided according to business requirements, and unnecessary access should be restricted.

Backup is another important control. A backup strategy should consider not only how often information is copied but also where backups are stored and whether they can be restored successfully. Regular testing is important because an organization may discover during an emergency that a backup cannot be recovered.

Data protection is consequently both a security issue and a business continuity issue.

6. CLOUD COMPUTING AND THIRD-PARTY RISK

Cloud computing has changed the way organizations acquire and manage technology. Instead of maintaining all infrastructure internally, organizations can use external providers for computing, storage, software and other services.

Cloud services can provide flexibility and support continuity, particularly when employees need to work from different locations. However, they also create new dependencies.

An organization may have limited direct control over the physical infrastructure supporting its services. It therefore needs to understand the provider's security arrangements, availability commitments, recovery capabilities and incident-reporting procedures.

Third-party risk should be included within the organization's overall technology risk framework. Before relying on an important technology supplier, organizations should consider its financial stability, security controls, service availability, data-handling practices and recovery arrangements.

Contracts should also clearly establish responsibilities. An organization should understand which risks remain its responsibility even when technology services are outsourced.

7. HUMAN FACTORS IN TECHNOLOGY RISK

Technology risk is often discussed in terms of systems and infrastructure, but employees are equally important.

Human error can result in data loss, security incidents and operational failures. Employees may accidentally delete information, disclose confidential material, click on malicious links or use technology incorrectly.

Training can reduce some of these risks. However, training should not be treated as a single annual activity. Technology and threats change continuously, so employee awareness needs regular reinforcement.

Management also has an important role. If employees are expected to follow security procedures but management ignores those procedures when they become inconvenient, the organization can develop a weak security culture.

A strong technology risk culture requires employees to understand that technology risk is part of their everyday responsibilities.

8. RISK IDENTIFICATION AND ASSESSMENT

Effective technology risk management begins with identifying important technology assets and dependencies.

Organizations should ask several basic questions:

- Which technology systems are essential to operations?
- Which information is critical?
- Which systems depend on external providers?
- What could cause these systems to fail?
- What would happen if a system became unavailable?
- How long could the organization operate without it?
- What controls are already in place?
- Where are the main weaknesses?

Risk assessment can then be used to prioritize risks according to their likelihood and potential impact.

Not every technology risk requires the same response. High-impact risks may require immediate attention, while lower risks can be monitored or accepted.

This prioritization is important because organizations have limited financial and human resources. Risk management should direct resources toward areas where they can provide the greatest reduction in potential harm.

9. RISK TREATMENT AND CONTROLS

Once technology risks have been identified and assessed, organizations need to determine how they will be treated.

Four common approaches are:

1. **Avoidance** – stopping an activity that creates an unacceptable risk.
2. **Reduction** – implementing controls to reduce likelihood or impact.
3. **Transfer** – transferring part of the financial or operational consequences through contracts or insurance.
4. **Acceptance** – deliberately accepting a risk when further controls are not justified.

Technology controls may include access management, encryption, network protection, backups, system redundancy, monitoring, patch management and incident-response procedures.

However, controls should be proportionate to the importance of the system. Applying expensive controls to a low-impact system may not be an efficient use of resources.

10. MONITORING AND CONTINUOUS IMPROVEMENT

Technology risk changes over time. New vulnerabilities emerge, employees change roles, systems are upgraded and organizations become dependent on new suppliers.

For this reason, technology risk management should include continuous monitoring.

Organizations should regularly review:

- security incidents
- system failures
- vulnerabilities
- supplier performance
- backup and recovery results
- employee awareness
- technology changes
- emerging threats

Testing is particularly important. Organizations can conduct simulated cyber incidents, disaster-recovery exercises and system recovery tests to identify weaknesses before a real event occurs.

Lessons from incidents and exercises should then be incorporated into future risk assessments and continuity plans.

This creates a cycle of:

Identify → Assess → Treat → Monitor → Learn → Improve

Such a cycle supports both technology risk management and organizational resilience.

11. DISCUSSION

The literature suggests that technology risk management should move beyond a narrow focus on preventing technical failures. Technology is now integrated into almost every major organizational function, meaning that technology risks can quickly become strategic and operational risks.

A useful approach is therefore to connect technology risk management with enterprise risk management, business continuity and organizational resilience.

This integration can help senior managers understand the consequences of technology decisions in business terms. For example, rather than asking only whether a system is technically secure, management should also ask what would happen to customers, revenue, employees and critical operations if the system became unavailable.

Research by Li, Cheng and Lu (2024) supports the importance of organizational technology capabilities for resilience. Their findings indicate that IT infrastructure, human capability and alignment between IT and business strategy can contribute to organizational resilience.

This reinforces the idea that technology risk is not solely the responsibility of IT specialists. Senior management, risk professionals, operational departments and employees all have a role.

12. CONCLUSION

Technology has created significant opportunities for organizations, but it has also introduced new forms of risk. Cybersecurity incidents, system failures, data loss, third-party dependencies and technological change can disrupt important activities and create substantial consequences.

Technology risk management provides organizations with a structured way to understand and manage these risks. Effective risk management requires organizations to identify critical systems and information, assess potential threats, establish appropriate controls, monitor changing conditions and learn from incidents.

The most important conclusion is that technology risk should be treated as an organizational issue rather than simply an IT issue. Technical controls are necessary, but they are most effective when supported by appropriate policies, employee awareness, management involvement and business continuity arrangements.

Organizations that integrate technology risk management with resilience and continuity planning are better positioned to deal with unexpected events. Rather than attempting to eliminate all technology risks, organizations should develop the capability to understand, prioritize and manage them while maintaining critical activities when disruption occurs.

REFERENCES

- [1] Bhamra, R., Dani, S., & Burnard, K. (2011). Resilience: The concept, a literature review and future directions. *International Journal of Production Research*, 49(18), 5375–5393.
- [2] Duchek, S. (2020). Organizational resilience: A capability-based conceptualization. *Business Research*, 13, 215–246. <https://doi.org/10.1007/s40685-019-0085-7>
- [3] Galaitsi, S. E., Pinigina, E., Keisler, J. M., Pescaroli, G., Keenan, J. M., & Linkov, I. (2023). Business continuity management, operational resilience, and organizational resilience: Commonalities, distinctions, and synthesis. *International Journal of Disaster Risk Science*, 14, 713–721.

- [4] Herbane, B. (2010). Small business research: Time for a crisis-based view. *International Small Business Journal*, 28(1), 43–64.
- [5] ISO. (2019). *ISO 22301:2019 Security and resilience—Business continuity management systems—Requirements*. International Organization for Standardization.
- [6] Li, M., Cheng, S., & Lu, M. (2024). Impact of information technology capabilities on organizational resilience: The mediating role of social capital. *Humanities and Social Sciences Communications*, 11, 1424.
- [7] Linnenluecke, M. K. (2017). Resilience in business and management research: A review of influential publications and a research agenda. *International Journal of Management Reviews*, 19(1), 4–30.
- [8] Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors*, 23(15), 6666.
- [9] Sahebjamnia, N., Torabi, S. A., & Mansouri, S. A. (2015). Integrated business continuity and disaster recovery planning: Towards organizational resilience. *European Journal of Operational Research*, 242(1), 261–273.
- [10] Sheffi, Y., & Rice, J. B. (2005). A supply chain view of the resilient enterprise. *MIT Sloan Management Review*, 47(1), 41–48.