RCMOS – Revista Científica Multidisciplinar O Saber | ISSN 2675-9128
Year VII, Vol. 2 (2026) | Submitted: 14 Jan 2026 | Accepted: 17 Jan 2026 | Published: 20 Jan 2026

Technology Resilience in Small and Medium-Sized Enterprises: Business Continuity, Backup and IT Environment Recovery

Guilherme Gallo Zazeri

Information Technology professional, consultant, and entrepreneur specializing in infrastructure, connectivity, and technology solutions, with more than 25 years of professional experience.

Abstract

The growing dependence on servers, cloud services, networks, and applications has made technology continuity a basic operating condition for small and medium-sized enterprises. This article examines IT resilience through critical-asset identification, business impact analysis, backup strategies, restoration testing, documentation, and monitoring. The study adopts a structured narrative review of verifiable standards, technical guides, books, and institutional reports, with emphasis on NIST CSF 2.0, NIST SP 800-34 Rev. 1, ISO 22301, and the Verizon DBIR. The analysis shows that possessing data copies is not equivalent to possessing recovery capability: continuity depends on defined priorities, responsibilities, protected copies, periodic tests, and executable procedures. For SMEs, the central challenge is to build controls proportional to risk and operational capacity, avoiding both lack of planning and unnecessarily complex architectures.

Keywords: technology resilience; business continuity; backup; disaster recovery; small and medium-sized enterprises; IT infrastructure.

1. Introduction

Technology infrastructure has ceased to be merely an administrative support function and has become part of the daily operations of companies in virtually every sector. Management systems, files, email, communication, remote access, and cloud services form chains of dependencies in which a technical failure can interrupt sales, customer service, billing, or production. Whitman and Mattord (2021) observe that information security must be addressed in connection with organizational objectives rather than as an isolated activity of the technical department.

For small and medium-sized enterprises, this dependence often coexists with small teams and heterogeneous environments. In 2024, NIST published a guide specifically for small businesses based on Cybersecurity Framework 2.0, recognizing that organizations with limited resources also need to structure governance, identification, protection, detection, response, and recovery (ELIOT, 2024). The question, therefore, is not to reproduce the architecture of a large corporation but to establish priorities consistent with risk.

Business continuity is one such priority. Swanson et al. (2010), in NIST SP 800-34 Rev. 1, link impact analysis, preventive controls, recovery strategies, testing, and maintenance to a consistent contingency program. On this basis, this article examines six dimensions of technology resilience in SMEs, with particular attention to the actual ability to restore services following failures, incidents, or outages.

2. Methodology

Open Access · Creative Commons Attribution · Cite the original work when reusing.

The study uses a structured narrative review, appropriate for integrating technical standards, information security literature, business continuity, and recent institutional evidence. Priority was given to sources with identifiable authorship, responsible institution, edition, and content.

The normative foundation consists of the NIST Cybersecurity Framework 2.0, NIST SP 1300 for small businesses, NIST SP 800-34 Rev. 1, and ISO 22301:2019. These references make it possible to distinguish risk management, organizational continuity, and systems recovery.

The works of Whitman and Mattord (2021) and Stallings (2018) were used to contextualize security, governance, and controls. The Verizon Data Breach Investigations Report 2025 was used as a contemporary empirical source on incidents and breaches.

The selection was not guided by commercial brands of hardware, hypervisors, or cloud services. The objective was to preserve applicability across different technology environments and prevent architectural recommendations from being confused with vendor preferences.

The materials were organized into six areas: criticality, impact analysis, backup, recovery, documentation, and monitoring. In each area, the aim was to distinguish the existence of a technical resource from demonstrated operational capability.

The article does not propose certification, auditing, or a universal continuity model. Recommendations must be adapted to each organization’s size, sector, regulatory requirements, budget, tolerance for downtime, and data criticality.

3.1 Technology Dependence and Asset Criticality

A resilience strategy begins by identifying what actually sustains operations. NIST CSF 2.0 (PASCOE; QUINN; SCARFONE, 2024) includes the Identify function precisely because organizations need to understand assets, dependencies, and risks before selecting controls.

Technical inventories gain value when linked to business processes. A server may appear to be merely a piece of equipment but may host authentication, files, or an application essential to billing. Criticality should be defined by the impact of unavailability, not by the price of the asset.

Swanson et al. (2010) link Business Impact Analysis to the determination of recovery priorities. The analysis helps identify which systems support essential functions and how much loss of availability can be tolerated.

In SMEs, hidden dependencies are common: credentials held by a single person, undocumented equipment, or legacy applications whose integration is not understood. Technical documentation reduces this risk by transforming tacit knowledge into organizational information.

Classification also prevents waste. Not all services require the same level of redundancy or the same recovery time. Stallings (2018) emphasizes that controls should be selected on the basis of risk, allowing resources to be concentrated on the most important components.

Thus, mapping criticality is a management decision. Infrastructure ceases to be a collection of devices and comes to be understood as a set of dependencies supporting business outcomes.

Open Access · Creative Commons Attribution · Cite the original work when reusing.

3.2 Impact Analysis, RTO, and RPO

Recovery planning must answer two questions: how long can the organization withstand the loss of a given service, and how much data can it afford to lose? Swanson et al. (2010) link these decisions to impact analysis and recovery objectives.

The Recovery Time Objective represents the target period for restoring a function or system. The Recovery Point Objective indicates the amount of data, measured in time, that the organization can accept losing. Although these concepts are technical, defining them depends on business decisions.

A very short RTO may require redundancy, automation, and additional infrastructure. An RPO close to zero may demand frequent or continuous replication. Recovery objectives must therefore be compatible with impact and budget.

ISO 22301 (2019) reinforces that continuity must be structured around organizational needs and the organization's capacity to respond to disruptions. This prevents decisions from being made solely on the basis of technical convenience.

Dependencies between systems must also be considered. Restoring an application without its database, authentication, or connectivity may not restore service to the user. The recovery sequence must reflect these relationships.

RTO and RPO therefore serve as a bridge between management and technology. When realistically defined, they guide backup, redundancy, contracts, testing, and investment priorities.

3.3 Backup Is Not Synonymous with Recovery

Backup is one component of recovery, but its mere existence does not guarantee continuity. NIST SP 800-34 Rev. 1 states that effective backup processes are crucial to the recovery strategy and links their frequency to needs identified through impact analysis (SWANSON et al., 2010).

A copy may fail because of corruption, incorrect configuration, compromised credentials, or insufficient retention. Backup management must therefore consider coverage, frequency, integrity, protection, and restoration capability.

Whitman and Mattord (2021) treat availability as a central dimension of information security. This perspective shows that protecting data includes ensuring that it can be recovered when needed.

Logical or physical separation of copies reduces the possibility that a single incident will compromise both production and backup simultaneously. The appropriate design depends on the environment, but the principle is to avoid single points of failure.

Retention policies must also account for versions. An accidental deletion or malicious alteration may be discovered days later; if all copies already reflect the compromised state, the backup loses part of its usefulness.

The relevant question, therefore, is not merely whether backup exists, but whether the organization knows what is protected, how far back it can recover, and how long recovery would take.

Open Access · Creative Commons Attribution · Cite the original work when reusing.

3.4 Restoration Testing and Demonstrated Capability

Testing recovery transforms an expectation into evidence. Swanson et al. (2010) include testing, training, and exercises among the stages of contingency planning precisely because plans that have never been executed may contain incorrect assumptions.

A restoration test may reveal incomplete files, overlooked dependencies, unavailable passwords, or recovery times incompatible with the established objective. Such problems are less costly when discovered before an emergency.

Testing frequency should reflect criticality and the pace of change. Systems that are frequently modified may require more frequent validation. Stable environments still need testing because hardware, software, credentials, and people change over time.

Exercises also evaluate communication. Recovery involves deciding who authorizes, who executes, who validates, and who informs users or customers. ISO 22301 (2019) treats organizational preparedness as part of continuity, not merely technical restoration.

Test results must be documented. Observed time, failures identified, corrective actions, and responsible parties make it possible to track progress and demonstrate that the plan is maintained.

Recovery capability is therefore better expressed through testing evidence than through the number of tools installed. Resilience is a demonstrated operational property, not a promise.

3.5 Documentation and Reducing Dependence on Individual Knowledge

IT environments accumulate informal knowledge: addresses, credentials, firewall rules, topologies, routines, and exceptions. When this information is concentrated in one person, the team itself becomes a single point of failure.

NIST CSF 2.0 (2024) places greater emphasis on governance and communication of responsibilities. Documenting assets, procedures, and decisions helps organizations maintain controls even when personnel change.

Useful documentation does not need to be extensive. Up-to-date inventories, network diagrams, dependency lists, contacts, recovery procedures, and secure credential storage locations may provide more value than long, outdated manuals.

Version control is equally important. An old diagram may lead to incorrect decisions during an incident. Documentation should be part of the change process rather than being updated only when an audit or failure occurs.

Stallings (2018) links policies and procedures to consistent security implementation. In continuity, documentation performs a similar function: it enables critical actions to be repeated predictably.

Reducing dependence on individuals also facilitates training and knowledge transfer. In this sense, technology resilience includes the ability to preserve operational knowledge beyond the people who originally configured the environment.

Open Access · Creative Commons Attribution · Cite the original work when reusing.

Year VII, Vol. 2 (2026) | Submitted: 14 Jan 2026 | Accepted: 17 Jan 2026 | Published: 20 Jan 2026

3.6 Monitoring, Prevention, and the Resilience Cycle

Monitoring makes it possible to identify degradation before it becomes an outage noticed by users. Storage capacity, service failures, connectivity loss, and backup errors are examples of signals that can be tracked.

NIST CSF 2.0 organizes risk management into Govern, Identify, Protect, Detect, Respond, and Recover. This structure shows that recovery is not an isolated stage: it depends on governance, environmental awareness, protection, detection, and coordinated response.

For SMEs, the value of monitoring lies in prioritization. Excessive alerts create noise; too few alerts leave failures invisible. Criticality and impact should guide which events require immediate action.

The Verizon DBIR 2025 analyzed more than 22,000 incidents and 12,195 confirmed breaches, reporting increased vulnerability exploitation and third-party involvement. This context reinforces the need to combine availability and security within a single operational discipline.

Monitoring must also cover the protection mechanism itself. A backup routine that stops running should trigger an alert; otherwise, the failure may remain invisible until recovery is needed.

Resilience is therefore cyclical. Organizations identify risks, protect assets, detect deviations, respond, recover, and incorporate lessons learned into the next design of the environment.

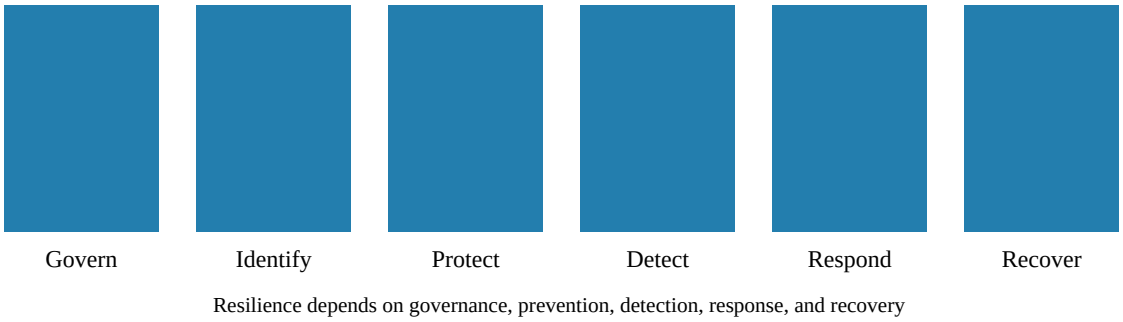


Figure 1. The six functions of the NIST Cybersecurity Framework 2.0. Source: prepared by the author based on Pascoe, Quinn, and Scarfone (2024).

3.7 Cost of Downtime and Proportionality of Investment

The discussion of resilience also has an economic dimension. Investments in backup, redundancy, and security compete with other priorities, especially in smaller companies. Therefore, the analysis should not begin with the idea of absolute protection, but with a comparison of potential impact, probability, and control cost. NIST CSF 2.0 (PASCOE; QUINN; SCARFONE, 2024) was designed precisely to enable organizations to prioritize security outcomes according to context and risk.

The cost of an interruption is not limited to replacing equipment. Unproductive hours, inability to issue invoices, delayed deliveries, data recovery, emergency hiring of specialists, and loss of trust can increase the financial impact. Whitman and Mattord (2021) link information security to the continuity of organizational functions, reinforcing the need to consider indirect impacts.

Open Access · Creative Commons Attribution · Cite the original work when reusing.

In 2025, an international survey released by Mastercard involving more than five thousand small and medium-sized business owners across four continents reported that 46% had experienced a cyberattack against their current business. Among those affected, nearly one in five said they had subsequently filed for bankruptcy or closed the company. This figure does not establish uniform economic causality, but it demonstrates the potential severity of incidents for organizations with less capacity to absorb losses.

The same Mastercard publication cites a 2024 estimate according to which the average cost of a cyberattack for companies with 25 to 299 employees reached US$250,000. Figures of this kind should not be automatically applied to every company, because industry, size, and type of incident affect the impact. They do, however, demonstrate why continuity and security must also be evaluated as financial decisions.

Proportional investment requires distinguishing essential controls from desirable solutions. An SME may achieve significant improvements through a reliable inventory, appropriate authentication, protected copies, tested restoration, system updates, and documentation before adopting highly complex architectures. Eliot (2024) reinforces this approach by directing the NIST guide to organizations with modest or nonexistent plans.

Technology resilience should thus be incorporated into business planning as exposure management. The economic objective is not to eliminate all risk, but to prevent a foreseeable failure from producing an impact disproportionate to the organization’s financial and operational capacity.

Conclusion

Technology continuity in small and medium-sized enterprises depends less on the number of tools than on consistency among risk, priority, and recovery capability. Mapping critical assets makes it possible to understand which dependencies sustain operations and prevents investments from being allocated without clear criteria.

Impact analysis turns downtime into decision-making parameters. RTO and RPO help align business expectations with technical design. Backups are indispensable, but they must not be confused with recovery. Integrity, retention, protection, and coverage must be verified.

Restoration tests provide the most concrete evidence that a plan can work. They also reveal dependencies and recovery times that do not appear in documents. Documentation reduces the risk of concentrated knowledge and facilitates continuity when teams, suppliers, or infrastructure change.

Monitoring connects prevention and response, allowing failures to be noticed before they produce greater impact and ensuring that protection mechanisms themselves are supervised. In conclusion, technology resilience is an organizational capability built continuously. For SMEs, proportionate, documented, and tested solutions can offer greater value than complex architectures that cannot be operated or recovered safely.

References

PASCOE, Cherilyn; QUINN, Stephen; SCARFONE, Karen. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. Gaithersburg: National Institute of Standards and Technology, 2024.

ELIOT, Daniel. NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide. NIST SP 1300. Gaithersburg: National Institute of Standards and Technology, 2024.

Open Access · Creative Commons Attribution · Cite the original work when reusing.

SWANSON, Marianne M.; BOWEN, Pauline; PHILLIPS, Amy W.; GALLUP, Dean; LYNES, David. Contingency Planning Guide for Federal Information Systems. NIST SP 800-34 Rev. 1. Gaithersburg: National Institute of Standards and Technology, 2010.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Security and Privacy Controls for Information Systems and Organizations. NIST SP 800-53 Rev. 5. Gaithersburg, 2020.

ISO. ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements. Geneva: International Organization for Standardization, 2019.

VERIZON. 2025 Data Breach Investigations Report. Basking Ridge, 2025.

STALLINGS, William. Effective Cybersecurity: A Guide to Using Best Practices and Standards. Boston: Addison-Wesley, 2018.

WHITMAN, Michael E.; MATTORD, Herbert J. Principles of Information Security. 7th ed. Boston: Cengage, 2021.

MASTERCARD. A small business expert answers your most pressing questions. 2025.