Capability Guide: Technology Resilience

Digital Work Must Be Secure, Available, and Recoverable.

Document Version 1.0 FINAL | TIO-KR-2026.08.0 | August 2026

Table of Contents

How to use this guide

Read Sections 1 through 3 for the executive view. Use Sections 4 through 7 to build and mature the capability. Use Section 8 to decide what to do next Monday morning.

01 Executive Brief

Technology Resilience is the organization's ability to keep critical digital services, platforms, integrations, automations, data pathways, and AI-enabled work secure, available, recoverable, and reliable.

Resilience is the fifth Technology capability. Architecture shapes. Platforms enable. Integration connects. Automation improves. Resilience protects. It makes sure the digital environment can be trusted when the organization depends on it.

Capability ID	T5 - Resilience
Domain	Technology
Plain-English test	Can the organization keep important digital services working, protected, monitored, recoverable, and improved when something changes, fails, or is attacked?
Five behaviors	Identify. Protect. Monitor. Respond. Recover.
Three outputs	Critical Digital Services Register. Resilience Standards and Recovery Plan. Resilience Health Review.
Accountable owner	Chief Information Officer, technology executive, security leader, service owner, or assigned technology leader, working with Risk, Governance, Data, Factory, and business owners.
First move	Identify the critical digital services, systems, integrations, automations, AI tools, data flows, and vendors the organization depends on most.

Core idea

Technology Resilience is the organization's ability to keep critical digital services, platforms, integrations, automations, data pathways, and AI-enabled work secure, available, recoverable, and reliable. As the organization becomes more digital and AI-aware, resilience becomes a business capability, not only an IT concern.

2026.08 ALIGNMENT | Resilience in the refreshed TIO system

Primary outcome contribution: Enterprise Autonomy

- Design intelligent and automated work to continue, degrade safely, stop, recover, reconcile, and change direction.
- Resilience includes model, provider, platform, data, identity, agent, workflow, and human fallback dependencies.
- Recovery evidence is a condition for expanding Delegated Autonomy and a practical test of Enterprise Autonomy.

Evidence at managed maturity: Resilience is defined, owned, applied consistently, measured in operation, reviewed through evidence, and improved without weakening trust, accountability, or Enterprise Autonomy.

First refresh move: Test how one intelligent workflow will stop, degrade safely, reconcile, and recover when a model, provider, data source, or integration fails.

02 The Problem This Capability Solves

Organizations now depend on digital work more than leaders often realize. Customer service, finance, operations, sales, reporting, compliance, employee productivity, automation, and AI-enabled work all rely on systems, data, access, networks, vendors, and integrations working together.

When digital work fails, the organization does not simply have an IT problem. Work stops. Decisions slow down. Customers are affected. Trust is damaged. People return to manual workarounds. Leaders lose confidence in technology and automation.

Technology Resilience solves this problem by making critical digital services visible, protected, monitored, recoverable, and regularly improved.

When Resilience is weak

- The organization does not know which digital services, data flows, automations, and vendors are truly critical.
- Important systems are available most of the time, but recovery expectations are unclear.
- Cybersecurity, reliability, backup, disaster recovery, and incident response are treated as separate technical topics instead of one business resilience concern.
- Automations and AI-enabled workflows depend on systems or data pathways that are not monitored or recoverable enough.
- Incidents surprise leaders because there is no simple view of service health, vulnerabilities, dependencies, and recovery readiness.
- Recovery plans exist, but they are not tested, owned, updated, or connected to the work that matters most.
- The organization scales digital work faster than it can protect and recover it.

03 What this Capability Is

Resilience is the practical ability to keep important digital work dependable. It includes security, availability, reliability, monitoring, backup, recovery, incident readiness, dependency visibility, and continuous improvement.

This capability is not only about technical uptime. It is about protecting the work, data, trust, service, and value that technology now supports. The more the organization uses AI, automation, data, and digital workflows, the more resilience matters.

What Resilience owns

- The technology view of critical digital services and dependencies.
- Standards for availability, monitoring, backup, recovery, incident response, and service health.
- Technical controls and operating practices that keep services secure, reliable, recoverable, and supportable.
- Recovery planning, testing, and lessons learned for critical digital services.
- Service health reporting, incident learning, and improvement actions for technology-supported work.
- Input into risk, governance, platform, integration, automation, data, and Factory decisions where resilience matters.

What Resilience does not own

- Enterprise risk appetite. Risk defines exposure, risk appetite, and trust requirements.
- Governance decision rights. Governance decides who can approve, stop, escalate, and review.
- Enterprise strategy. Strategy sets direction and priorities.
- Data ownership, quality, access, flow, and insight. Data owns the data capabilities.
- Business continuity for the whole organization. Resilience supports digital continuity, but the business owns how work continues.
- Every security policy. Risk, legal, privacy, security, and technology leaders share responsibility for protection.
- Factory delivery. Factory proves and scales AI Use Cases and work redesign. Resilience makes sure the digital services they depend on are dependable.

Five core behaviors

Behavior	What it means in practice
Identify	Know which digital services, systems, data flows, integrations, automations, AI tools, vendors, and dependencies matter most.
Protect	Apply the right security, access, backup, redundancy, and configuration controls based on importance and risk.
Monitor	Track service health, incidents, failures, vulnerabilities, dependency changes, and early warning signals.
Respond	Act quickly when something fails, is attacked, performs poorly, or creates service risk.
Recover	Restore critical digital services and learn from incidents, tests, failures, and near-misses.

04 How the Capability Works

Resilience should start with what matters most to the business. Not every system requires the same level of protection, monitoring, and recovery. Critical digital services need more discipline than low-impact tools.

Simple operating model

Step	Plain-English question
1. Identify critical digital services	Which systems, platforms, integrations, automations, data pathways, AI tools, and vendors are essential to the work?
2. Understand dependencies	What does each service depend on, including data, access, cloud services, vendors, integrations, networks, people, and support paths?
3. Set resilience expectations	How available, secure, monitored, and recoverable does this service need to be?
4. Apply controls	What protection, backup, monitoring, logging, access, recovery, and support controls are needed?
5. Monitor health	Can leaders and service owners see performance, incidents, vulnerabilities, failures, and service risk?
6. Test recovery	Have recovery plans been tested, updated, and connected to real business work?
7. Improve from evidence	What must change based on incidents, near-misses, tests, audits, vendor changes, and new digital work?

Resilience rule

Do not protect everything the same way. Start with the digital services the organization depends on most. Make them visible, protected, monitored, recoverable, and improved.

Boundary with Risk

Risk identifies what could go wrong, how serious it could be, who could be affected, and what level of exposure matters. Resilience keeps the critical digital services protected and recoverable enough to meet those expectations.

Risk says what level of trust must be protected. Resilience makes the digital environment dependable enough to protect it.

05 Outputs, Evidence, and Measures

Resilience should produce a small number of useful outputs. The goal is to make critical services visible, resilience expectations clear, and recovery readiness real.

Output	Purpose	What it contains	Quality standard
Critical Digital Services Register	Makes the digital services the organization depends on visible.	Service, owner, business process supported, users affected, dependencies, data used, vendor reliance, availability need, recovery need, security exposure, and current health.	Clear enough for leaders to know which services matter most and why.
Resilience Standards and Recovery Plan	Defines how critical digital services are protected, monitored, and recovered.	Availability expectations, backup approach, access controls, logging, monitoring, incident route, recovery steps, recovery owner, testing rhythm, and escalation path.	Practical enough to use during a real incident and simple enough to keep current.
Resilience Health Review	Keeps service health, incidents, recovery readiness, and improvement actions visible.	Service status, incidents, vulnerabilities, failed backups, recovery tests, dependency changes, open issues, vendor concerns, and improvement actions.	Used by technology and business leaders to make decisions, not just to report status.

Evidence that the capability exists

- Critical digital services and dependencies are documented and owned.
- Availability, security, monitoring, backup, recovery, and support expectations are defined for critical services.
- Recovery plans are tested and updated based on evidence.
- Incidents, near-misses, outages, vulnerabilities, failed backups, and vendor changes are reviewed and acted on.
- Material AI Use Cases, automations, integrations, and data flows are reviewed for resilience needs before they scale.
- Technology leaders can explain which digital services create the highest business exposure if they fail.

Useful measures

Measure	Why it matters
Percentage of critical digital services with named owner and recovery plan	Shows whether resilience accountability exists.
Recovery test completion and results	Shows whether recovery plans work in practice.
Incident frequency, severity, duration, and repeat causes	Shows whether the environment is becoming more dependable.
Backup success, restore success, and unresolved backup issues	Shows whether recovery is real, not assumed.
Critical vulnerabilities and aging open risks	Shows whether known exposure is being reduced.
Service health and availability for critical services	Shows whether the organization can depend on its digital environment.

06 Maturity: 0 to 5

Level	What it looks like	Evidence	Next move
0 Absent	Resilience is not meaningfully defined. Critical digital services are not clearly known, owned, protected, monitored, or recoverable.	No critical service view, recovery plan, service health review, owner model, or recovery testing.	Identify the most important digital services and name owners.
1 Initial	Some protection, backup, recovery, and incident practices exist, but they depend on individuals or technical teams.	Local backup practices, informal recovery knowledge, ad hoc incident response, and limited service visibility.	Create a simple critical digital services register and confirm current recovery assumptions.
2 Repeatable	Basic resilience practices are used for priority systems and services.	Named owners, basic monitoring, backup checks, incident route, recovery plan, and limited testing for some critical services.	Define resilience standards and recovery expectations for all critical digital services.
3 Defined	Resilience is documented, owned, communicated, and used consistently for critical digital services.	Critical service register, resilience standards, recovery plans, testing rhythm, incident review, and service health review.	Measure service health, recovery performance, vulnerabilities, repeat incidents, and improvement actions.
4 Managed	Resilience is measured, governed, improved, and connected to risk, governance, data, automation, AI Use Cases, and business continuity.	Health review pack showing service status, incidents, test results, open issues, vulnerabilities, recovery readiness, and decisions.	Use evidence to improve designs, reduce weak points, and strengthen priority services.
5 Optimized	Resilience continuously improves as strategy, platforms, data, automation, AI, vendors, threats, and business needs change.	Resilience is built into digital decisions, platform choices, use case scaling, vendor management, and operating reviews.	Keep resilience adaptive so the organization can move faster without becoming fragile.

07 How to Build and Mature the Capability

Start with the digital services that matter most. The organization does not need a perfect resilience model on day one. It needs a practical view of the systems, platforms, integrations, data pathways, automations, AI tools, and vendors that would seriously disrupt work if they failed.

Minimum viable Resilience capability

- A simple register of critical digital services and dependencies.
- A named service owner for each critical service.
- Basic availability, protection, monitoring, backup, and recovery expectations.
- A practical recovery plan and escalation route for each critical service.
- A tested backup and recovery approach for services that matter most.
- A regular health review covering incidents, vulnerabilities, backups, recovery tests, vendor concerns, and open actions.
- Clear routing to Governance and Risk when resilience exposure exceeds accepted thresholds.

Timeframe	Practical actions
First 30 days	List the top critical digital services. Name owners. Identify the most important dependencies and current recovery assumptions. Confirm whether backups and recovery paths are known.
First 90 days	Create the critical services register, resilience standards, recovery plan template, incident route, and first health review. Test recovery for the most important service or data pathway.
First 12 months	Expand recovery testing, improve monitoring, close known weak points, connect resilience to AI Use Cases and automations, and review service health with business leaders.

What not to build too early

- A complex resilience program before critical services are known and owned.
- Recovery plans that are never tested.
- Technical dashboards that business leaders cannot understand or use.
- Security, recovery, incident, vendor, and service health practices that are disconnected from each other.
- AI and automation scaling that depends on fragile systems, unknown data paths, or untested recovery plans.
- A belief that cloud, vendors, or managed services remove the organization's responsibility for resilience.

08 TSLA Support and First Moves

The organization must own its digital resilience. TSLA can help leaders make resilience understandable, business-connected, and aligned to TIO strategy, risk, governance, data, technology, Factory, and People decisions.

Where TSLA can help

Support area	Practical result
Critical Digital Services Review	A clear view of the systems, platforms, integrations, automations, AI tools, data pathways, and vendors the organization depends on most.
Resilience Standards and Recovery Plan	A practical set of expectations for availability, protection, monitoring, backup, recovery, incident response, ownership, and escalation.
Service Health Review	A simple executive review pack showing incidents, recovery readiness, vulnerabilities, open actions, and priority decisions.
AI and Automation Resilience Check	A review of whether priority AI Use Cases and automations depend on services, data flows, integrations, or vendors that are too fragile.
Governance and Risk Alignment	Clear routing for when resilience exposure needs a governance decision, risk review, investment decision, or leadership escalation.
Thought-Partnership	Ongoing executive support as resilience becomes more important to strategy, trust, digital work, and AI-enabled operations.

What to do Monday morning

- Ask which digital services would seriously disrupt the organization if they failed tomorrow.
- Create a simple list of the top ten critical systems, platforms, data pathways, automations, AI tools, and vendors.
- Name an owner for each critical digital service.
- Ask when each critical service was last recovered, not just backed up.
- Identify the most important dependencies and weak points.
- Review the last three incidents or outages and ask what was learned.
- Choose one critical service and test whether its recovery plan actually works.

A Source Note

This guide is part of the TIO Library. It is aligned to the TIO Framework, the TIO Technology Capability Domain Master, the TIO Capability Model and Maturity Assessment Tool, and the approved 8-section Capability Guide structure used across the TIO Library. It translates the Technology Resilience capability into practical guidance for leaders and practitioners.

It is written as a practical executive guide. It is not a technical data-management standard, legal opinion, privacy assessment, cybersecurity review, or professional assurance report. Organizations should apply their own policies, obligations, accountabilities, and professional review where required.