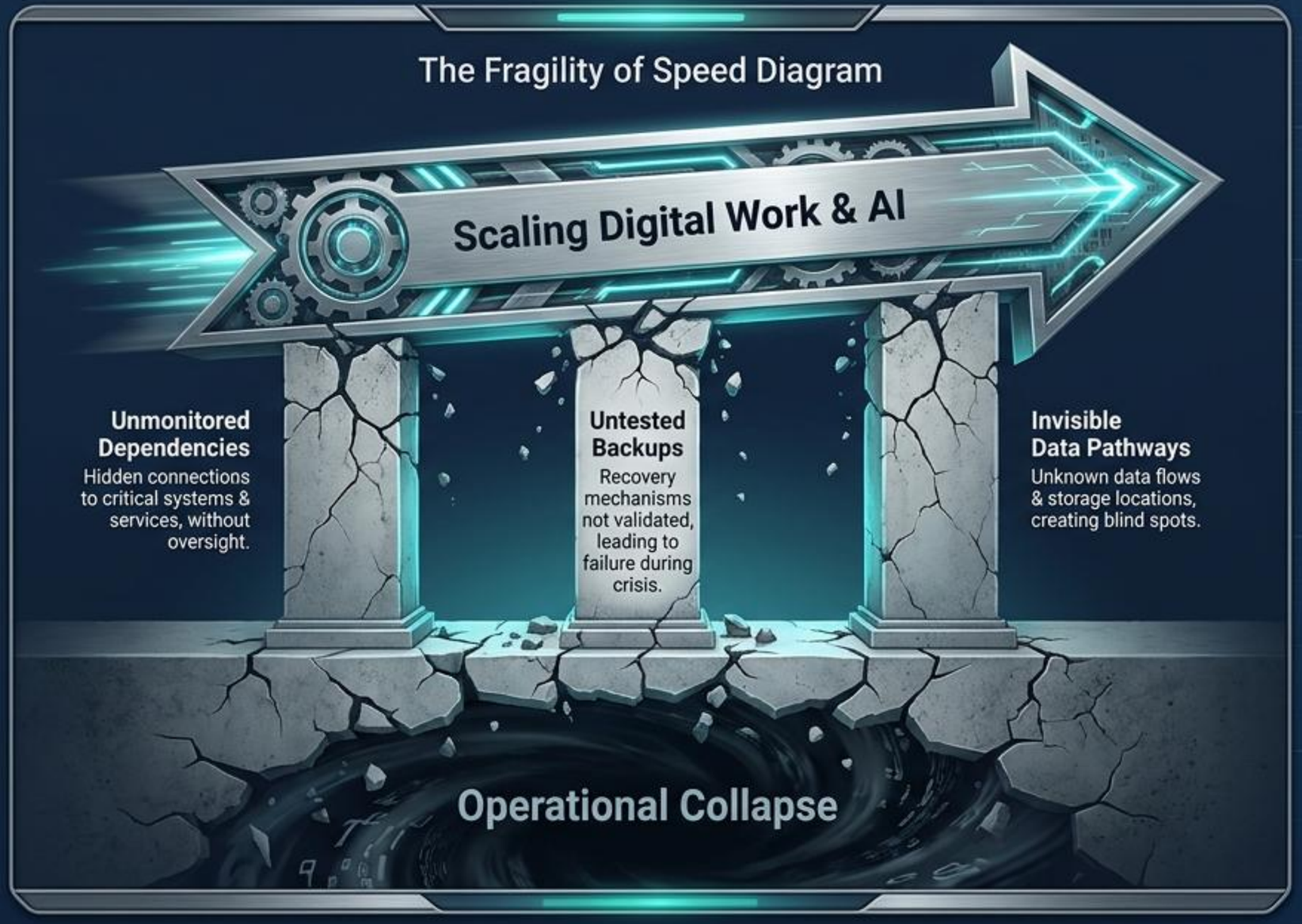
TIO Domain 3 (Technology) | Capability 5

Resilience: The Shield

Digital Work Must Be Secure, Available, and Recoverable.

The Intelligent Organization (TIO) Framework

Speed Without Resilience is Fragility



The Reality

The more an organization uses AI, automation, and digital workflows, the more resilience matters. This is no longer just an IT uptime concern; it is a fundamental business capability.

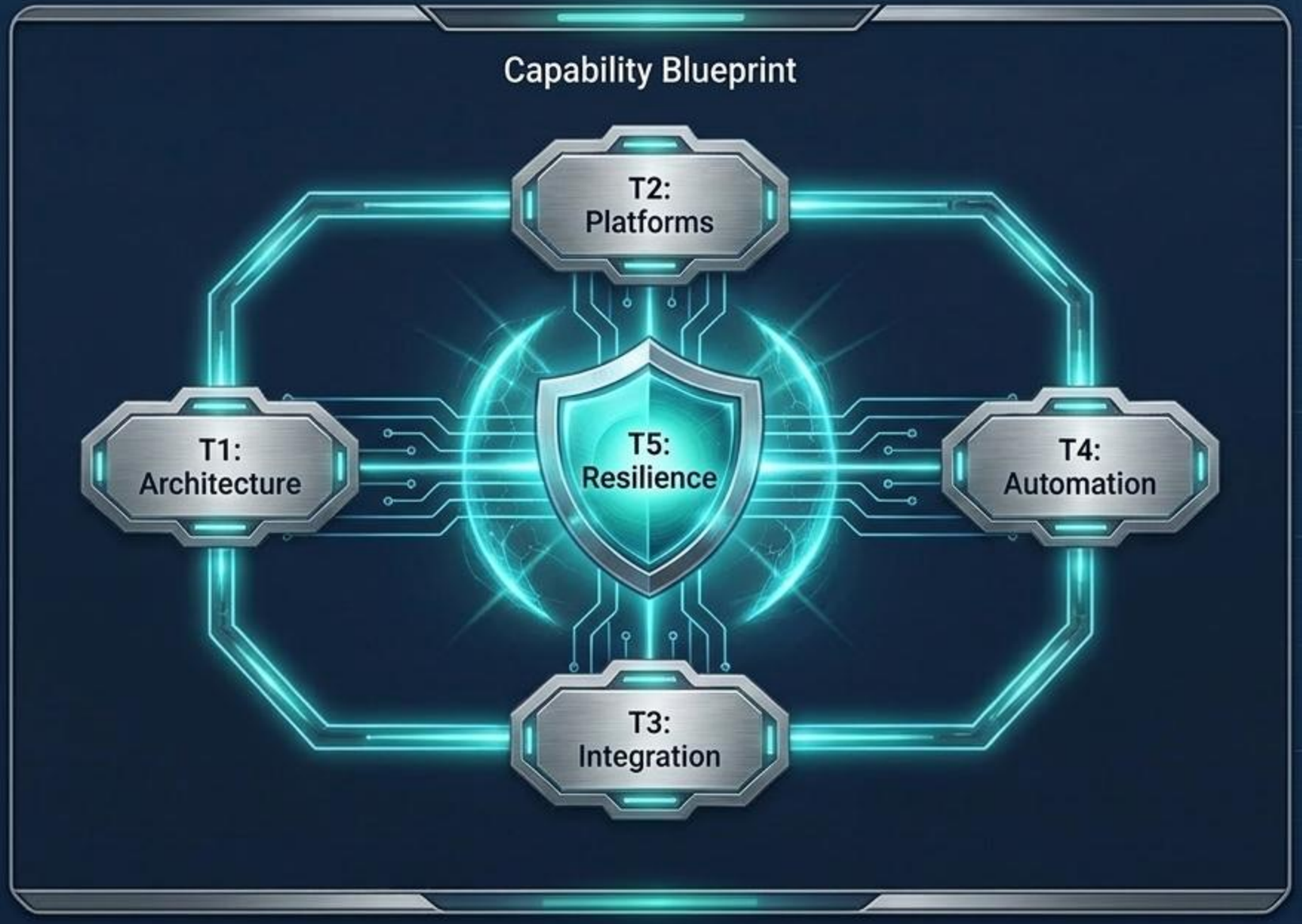
The Catastrophe of Surprise

Incidents surprise leaders because there is no simple view of service health, vulnerabilities, and recovery readiness. Automations depend on systems that are not recoverable enough.

The TIO Solution

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

The Anatomy of Capability T5



Canonical Definition

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.

The Plain-English Test

Can the organization keep important digital services working, protected, monitored, recoverable, and improved when something changes, fails, or is attacked?

The Operating Logic

Architecture shapes. Platforms enable. Integration connects. Automation improves.
Resilience protects.

The Boundary Line: Eliminating Organizational Turf Wars

The Assessor

Leadership Domain - Risk

Role

Identifies what could go wrong, defines exposure levels, and sets trust requirements.

Action

Says what level of trust must be protected. Sets enterprise risk appetite.

The Shield

Technology Domain - Resilience

Role

Keeps the critical digital services protected and recoverable.

Action

Makes the digital environment dependable enough to actually meet those trust expectations. Applies technical controls.

Risk sets the expectation. Resilience executes the protection.

The 5 Core Behaviors of the Shield

5. Recover
Restore services and learn from tests and near-misses.

1. Identify:
Know which digital services and dependencies matter most.

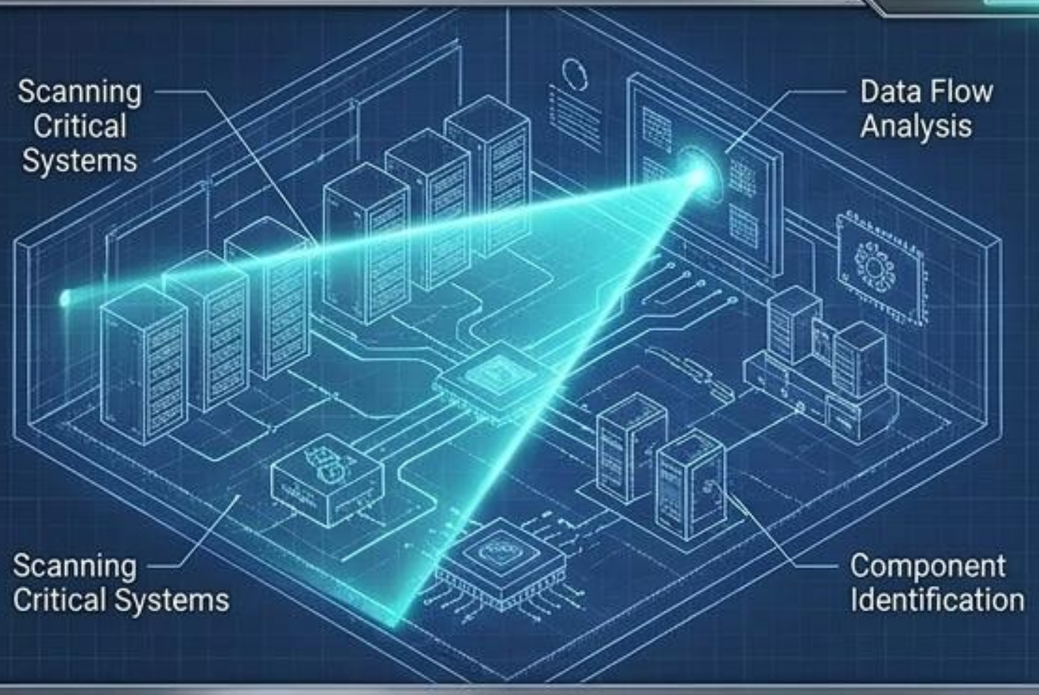
4. Respond:
Act quickly when something fails or is attacked.

2. Protect:
Apply the right security, access, and backup controls.

3. Monitor:
Track service health, vulnerabilities, and early warnings.

Core Rule: Do not protect everything the same way. Start with the digital services the organization depends on most.

Setting the Defensive Grid: Identify & Protect



1. **Identify** (Visibility is the Prerequisite)

- **The Action:** Find the critical systems, platforms, integrations, automations, data pathways, AI tools, and vendors essential to the work.
- **The Trap:** Blindly trusting that IT has it covered without knowing the business dependencies.

2. **Protect** (Proportionate Defense)

- **The Action:** Apply security, access, backup, redundancy, and configuration controls strictly based on importance and risk.
- **The Rule:** Critical digital services need more discipline than low-impact tools.

Active Defense: Monitor, Respond, Recover

3. Monitor (The Early Warning System)

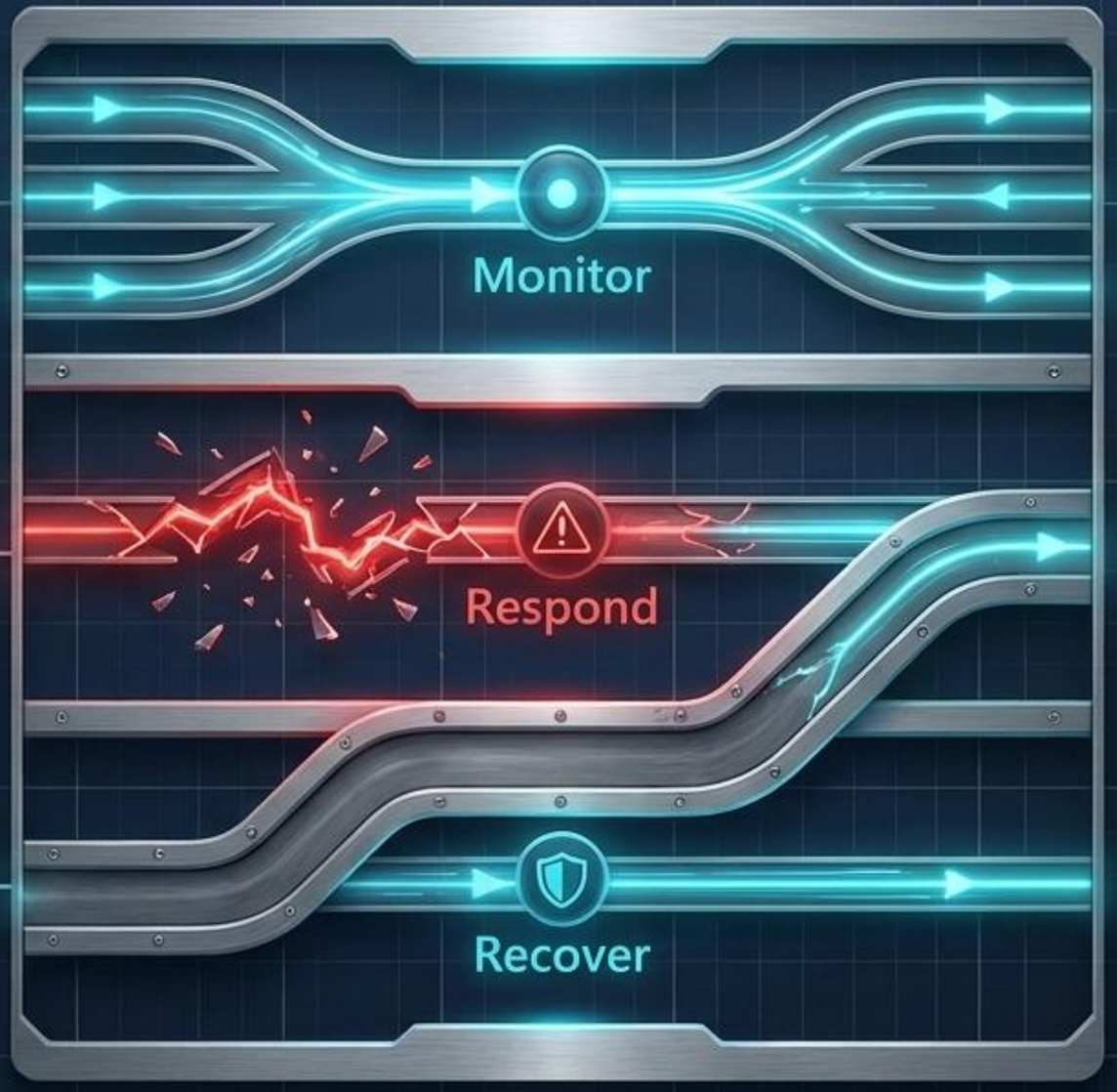
Track service health, incidents, failures, vulnerabilities, and dependency changes before they cause outages.

4. Respond (The Reflex)

Act decisively when a service fails, performs poorly, or creates exposure.

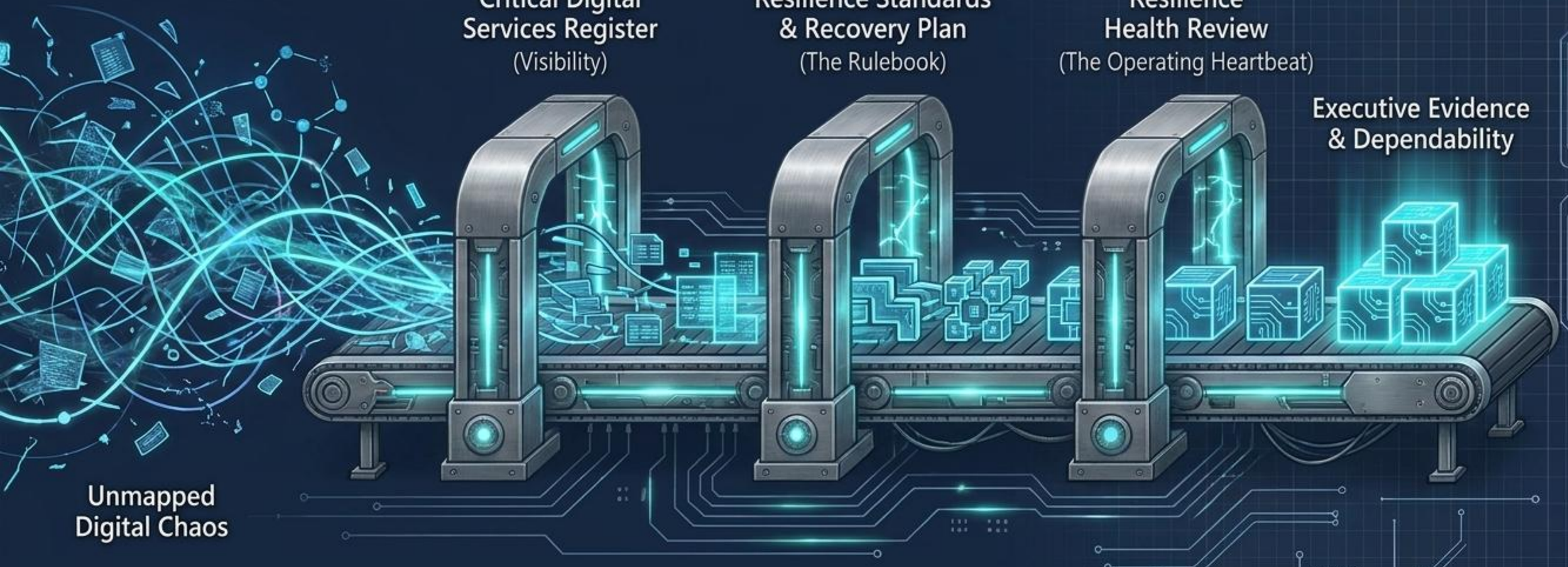
5. Recover (The Ultimate Test)

Restore critical digital services. Learn from incidents, tabletop tests, failures, and near-misses to update the shield.



The Architecture of Dependability: 3 Practical Outputs

Resilience produces a small number of useful outputs to make expectations clear and recovery readiness real.



Output 1: Critical Digital Services Register

The Purpose

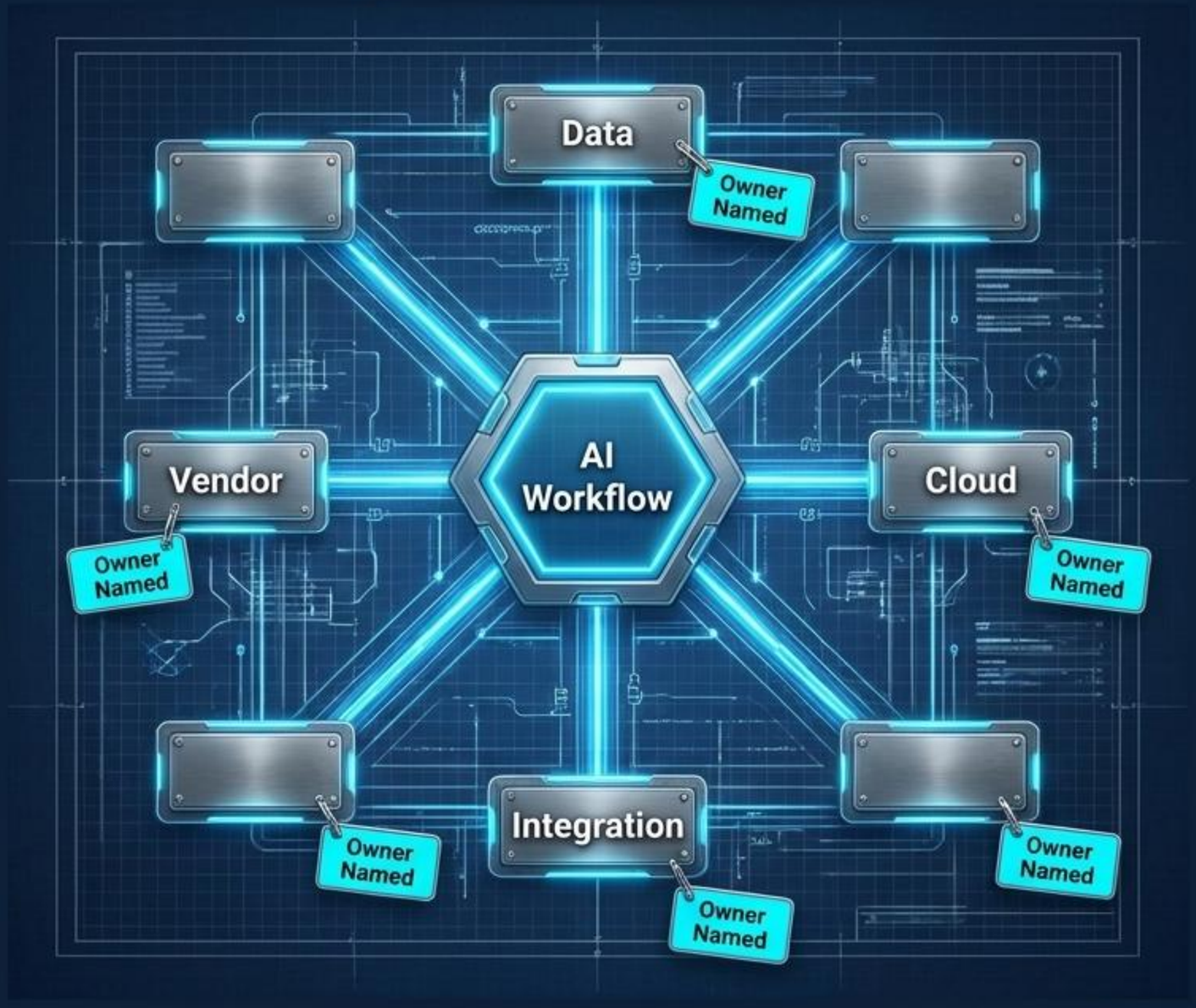
Makes the digital services the organization truly depends on visible.

What it Contains

Service, named owner, business process supported, dependencies, vendor reliance, availability need, and recovery need.

The Quality Standard

Must be clear enough for non-technical executives to immediately know which services matter most and why they pose a business risk if they fail.



Output 2: Resilience Standards & Recovery Plan

The Purpose

Defines exactly how critical digital services are protected, monitored, and brought back online.

What it Contains

Availability expectations, backup approach, access controls, logging, incident route, step-by-step recovery, and testing rhythms.

The Quality Standard

Practical enough to use during a real 2:00 AM incident, and simple enough to keep current. A recovery plan that has never been tested is just a theory.

Output 3: Resilience Health Review

The Purpose

Keeps service health, incidents, recovery readiness, and improvement actions continuously visible to leadership.

What Executives Look At:

- Service uptime vs. expectations.
- Unresolved backup failures.
- Recovery test results (pass/fail).
- Vendor risk changes.

The Rule: Used by technology and business leaders to make decisions, not just to report status.

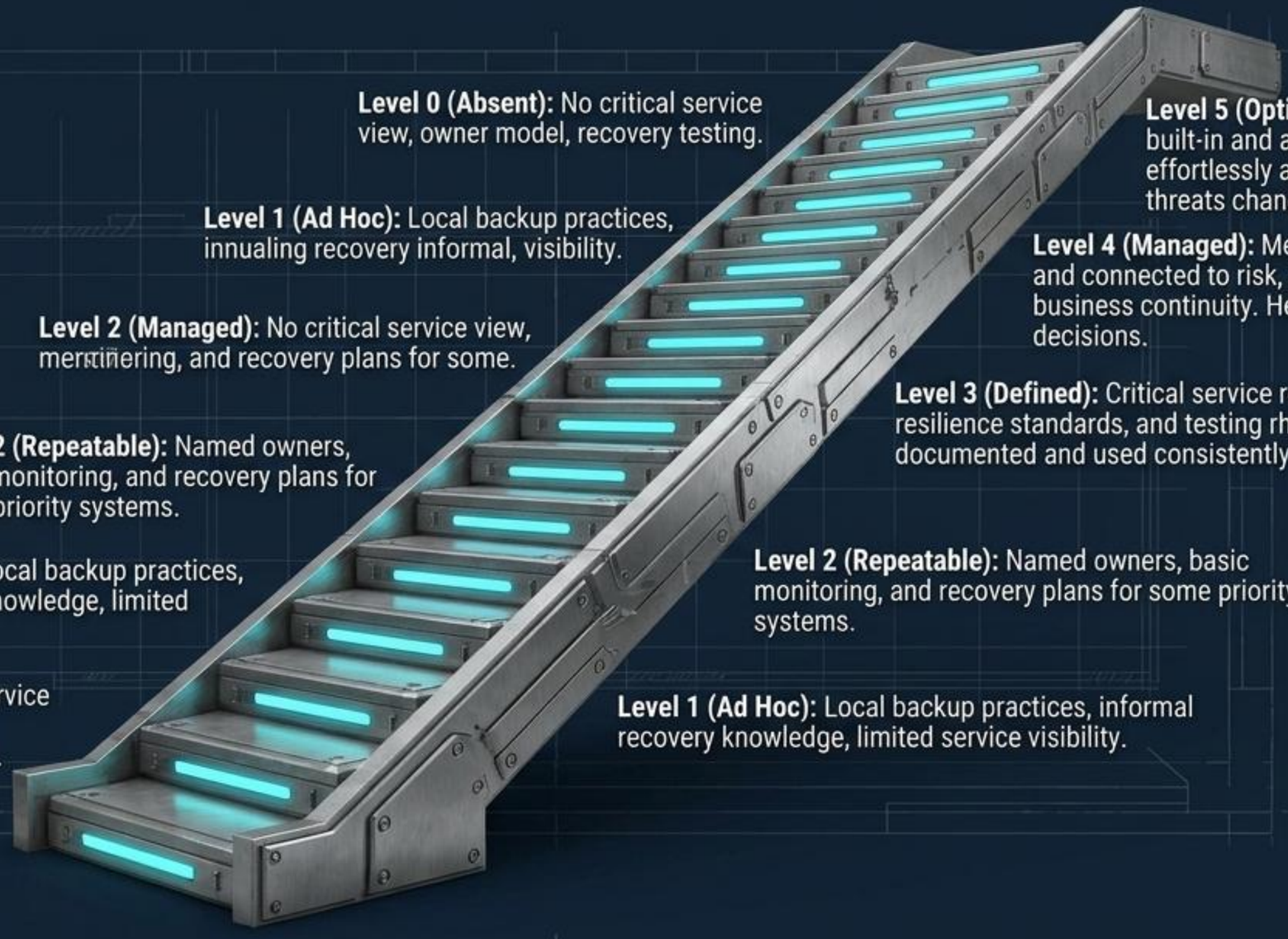
Synthesis: The Resilience Engine

Core Insight: These are not isolated tasks. The behaviors generate the outputs; the outputs govern the behaviors. It is a single, continuous engine.

Proving the Capability: Executive Evidence

The Litmus Test: Technology leaders can explicitly explain which digital services create the highest business exposure if they fail.

Measuring the Mandate: Where Are You?



Level 0 (Absent): No critical service view, owner model, recovery testing.

Level 1 (Ad Hoc): Local backup practices, innualing recovery informal, visibility.

Level 2 (Managed): No critical service view, mer[illegible]nering, and recovery plans for some.

Level 2 (Repeatable): Named owners, basic monitoring, and recovery plans for some priority systems.

Level 1 (Ad Hoc): Local backup practices, informal recovery knowledge, limited service visibility.

Level 0 (Absent): No critical service view, owner model, or recovery testing. Resilience is undefined.

Level 5 (Optimized): Resilience is built-in and adaptive. Scales effortlessly as platforms, AI, and threats change.

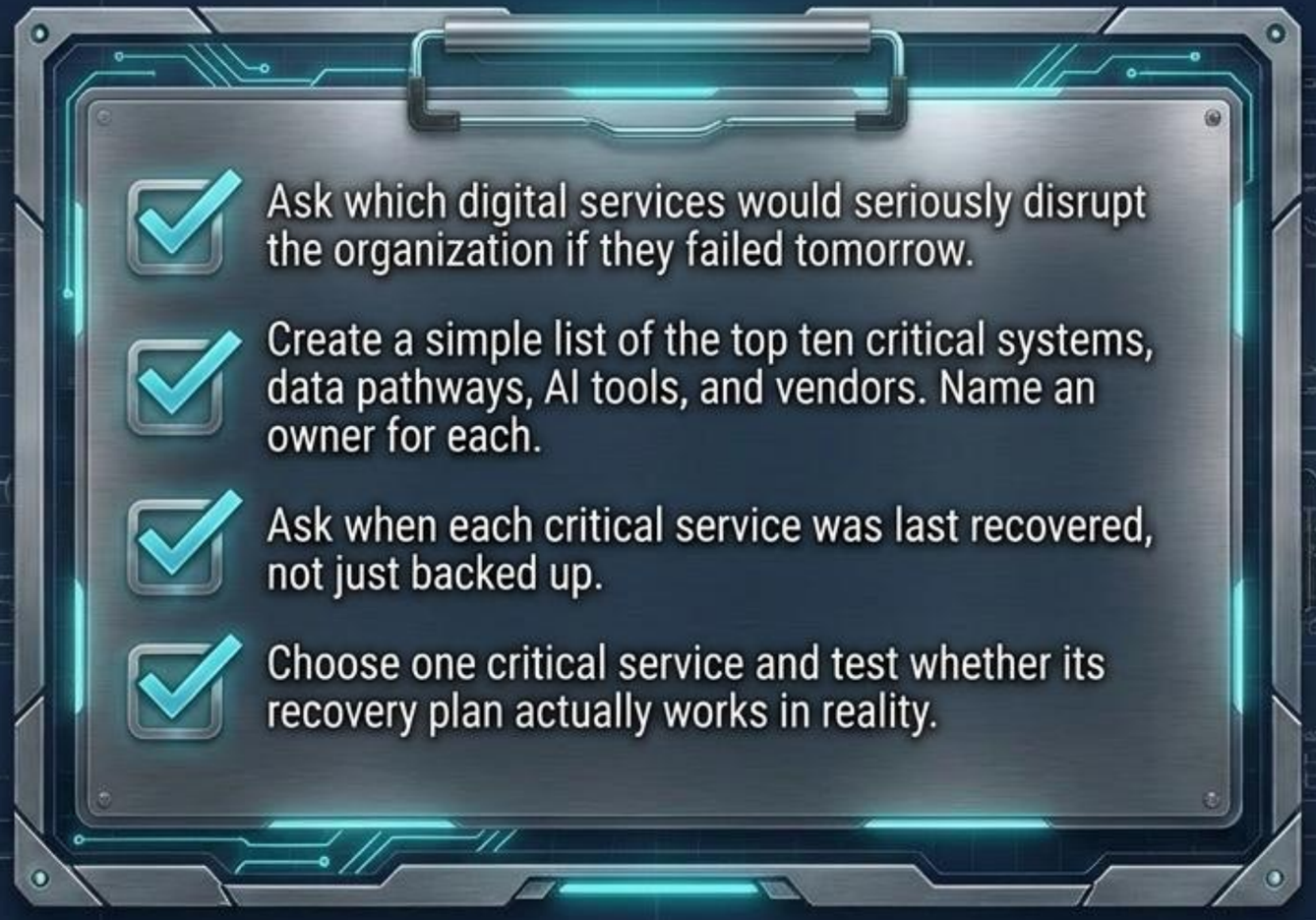
Level 4 (Managed): Measured, governed, and connected to risk, AI Use Cases, and business continuity. Health reviews drive decisions.

Level 3 (Defined): Critical service register, resilience standards, and testing rhythms are documented and used consistently.

Level 2 (Repeatable): Named owners, basic monitoring, and recovery plans for some priority systems.

Level 1 (Ad Hoc): Local backup practices, informal recovery knowledge, limited service visibility.

First Moves: What to do Monday Morning



- [x] Ask which digital services would seriously disrupt the organization if they failed tomorrow.
- [x] Create a simple list of the top ten critical systems, data pathways, AI tools, and vendors. Name an owner for each.
- [x] Ask when each critical service was last recovered, not just backed up.
- [x] Choose one critical service and test whether its recovery plan actually works in reality.

"As the organization becomes more digital and AI-aware, resilience becomes a business capability, not only an IT concern."