

5-Minute Identity Resilience & Recovery Readiness Assessment

Assess how prepared your organization is to recover identity fast, reverse unwanted changes, and reduce business disruption from identity outages.

Executive Context

AI-powered attacks are increasing the speed, scale, and impact of identity incidents. At the same time, organizations are deploying more AI agents, automation, service accounts, and nonhuman identities with elevated access across Active Directory, Entra ID, Microsoft 365, and Intune.

As change accelerates, identity risks that were once manageable at human speed can quickly become business continuity events. AI does not create every identity gap. It makes existing gaps harder to ignore by increasing the volume of permissions, automated actions, and opportunities for unintended changes. Organizations need confidence that they can identify what changed, reverse unwanted actions, and recover trusted identity services before a disruption becomes a prolonged outage.

Executive Context	1
Take the Assessment	1
Plot Your Position on the Executive Recovery Risk Matrix	2
Turn the Result Into an Executive Action Plan	3
Understand Your Low-Scoring Areas	3
About Cayosoft Guardian	7
Why Cayosoft	7

Take the Assessment

Purpose of Assessment

Determine whether the organization can recover identity fast enough to prevent extended business disruption, reverse risky or malicious changes, and restore trust across Active Directory, Microsoft Entra ID, Microsoft 365, and Intune.

How To Use This Assessment

Rate each statement from 1 to 4 based on today's operating reality. Then use the matching insight pages to understand low-scoring areas and identify where to start.

1 Unknown or unproven	2 Partly defined	3 Mostly validated	4 Executive-ready, tested, measured
---------------------------------	----------------------------	------------------------------	---

Area	Executive question	Rate
1. Identity RTO	Do we know the maximum identity downtime the business can tolerate for a forest-level or hybrid identity incident?	1 2 3 4
2. Clean Recovery Path	Can we recover identity without depending on compromised infrastructure, compromised credentials, or untrusted backups?	1 2 3 4
3. Ready Recovery Environment	Do we have a continuously validated standby recovery environment, or would we rebuild under pressure?	1 2 3 4
4. Forest Recovery Execution	Can we restore AD forest services through a controlled cutover instead of a manual, error-prone rebuild?	1 2 3 4
5. Rollback Capability	Can we quickly reverse risky or malicious changes to users, groups, policies, permissions, and configurations?	1 2 3 4
6. Hybrid Visibility	Can we see identity changes across AD, Entra ID, Microsoft 365, and Intune in one trusted timeline?	1 2 3 4
7. AI and Automation Change Control	Can we identify and reverse changes made by scripts, service accounts, automation, or AI agents?	1 2 3 4
8. Privileged Access Recovery	Can we restore and validate Tier-0 and privileged access without reintroducing attacker persistence?	1 2 3 4
9. Recovery Testing Evidence	Can executives see recent recovery-test evidence, not just a written disaster recovery plan?	1 2 3 4
10. Business Continuity Confidence	Can we explain the business impact of an identity outage and the plan to reduce downtime from days to minutes?	1 2 3 4

Plot Your Position on the Executive Recovery Risk Matrix

Use the 5×5 Executive Recovery Risk Matrix to translate assessment results into a board-ready business risk view. The goal is to move the organization toward the green zone by increasing recovery confidence while reducing the business impact of an identity outage.

Executive Recovery Risk Matrix

Business Impact ↓ / Recovery Confidence →	1 Unknown	2 Defined	3 Validated	4 Tested	5 Executive Ready
5 Severe	● Critical Exposure	● Critical Exposure	● High Risk	● Watch	● Watch
4 Major	● Critical Exposure	● High Exposure	● High Risk	● Watch	● Managed
3 Significant	● High Exposure	● High Risk	● Developing	● Managed	● Green
2 Minor	● High Risk	● Developing	● Managed	● Green	● Green
1 Insignificant	● Developing	● Managed	● Green	● Green	● Green

Placement by Assessment Score

Add the 10 ratings. Use the result as an executive conversation starter, not a formal maturity certification.

10 to 19: High recovery exposure

Critical identity recovery and rollback capabilities are missing, untested, or dependent on compromised infrastructure. Prioritize executive ownership, business-impact analysis, and a recovery modernization plan.

20 to 31: Developing recovery confidence

Important foundations exist, but gaps in clean recovery, rollback scope, hybrid visibility, or testing evidence could delay restoration during a major identity incident.

32 to 40: Executive-ready recovery posture

Most capabilities are validated. Continue testing the recovery path, documenting evidence, and confirming that rollback, privileged access, and hybrid dependencies stay aligned as the environment changes.

Turn the Result Into an Executive Action Plan

Board-level question: Can we restore identity access fast enough, cleanly enough, and confidently enough to prevent extended business disruption?

Priority gap: Identify the lowest-scoring area with the greatest business impact.

Business consequence: Estimate downtime, operational dependency, audit exposure, and recovery uncertainty.

Desired future state: Define the target RTO, clean recovery path, rollback scope, and evidence required for executive confidence.

Next step: Use the lowest-scoring areas to guide a Cayosoft Guardian demonstration or proof of concept focused on recovery, rollback, and hybrid identity resilience.

How Cayosoft Guardian Helps Move You to the Green Zone

- **Reduce identity recovery time from days to minutes** with continuously validated standby recovery environments powered by Guardian Instant Forest Recovery.
- **Minimize business disruption during identity incidents** through rapid rollback and change reversal with Guardian Audit & Restore.
- **Accelerate investigations and improve executive reporting** with unified visibility across Active Directory, Entra ID, Microsoft 365, and Intune through Guardian Change Monitoring.
- **Increase executive confidence in operational resilience** by enabling organizations to move from high recovery exposure to an executive-ready recovery posture with Guardian Identity Recovery.

Understand Your Low-Scoring Areas

For every item scored 1 or 2, use the guide below to frame the business risk, the required executive conversation, and the related Guardian resource.

1. Identity RTO

SECTION	CONTENT
THE PROBLEM	The organization has not defined or validated the maximum amount of identity downtime the business can tolerate.
WHY IT MATTERS	Without a target recovery objective, recovery efforts become reactive, recovery investments are difficult to prioritize, and business disruption can extend beyond acceptable limits.
HOW CAYOSOFT GUARDIAN HELPS	Guardian helps organizations establish and achieve identity recovery objectives by providing continuously validated recovery environments and rapid recovery capabilities.
LEARN MORE	Identity Recovery and Forest Recovery Protection

2. Clean Recovery Path

SECTION	CONTENT
THE PROBLEM	Recovery plans depend on infrastructure, credentials, or backups that may have been compromised during the incident.
WHY IT MATTERS	Restoring from compromised assets can reintroduce attacker persistence, malware, or configuration issues into the environment.
HOW CAYOSOFT GUARDIAN HELPS	Guardian provides an isolated and continuously validated recovery path designed to reduce reinfection risk.
LEARN MORE	Active Directory Forest Recovery: Strategies for 2026

CUSTOMER PROOF

“Cayosoft gives us peace of mind. We know we can recover in minutes, not days.

Director of IT Security, State of New Mexico

3. Ready Recovery Environment

SECTION	CONTENT
THE PROBLEM	Recovery environments must be built during the crisis instead of being maintained and validated in advance.
WHY IT MATTERS	Building recovery infrastructure under pressure increases downtime, introduces errors, and delays restoration of business operations.
HOW CAYOSOFT GUARDIAN HELPS	Guardian maintains a continuously validated standby recovery environment ready for controlled cutover when needed.
LEARN MORE	Guardian Instant Forest Recovery Now Supports WORM Storage for Azure and AWS

4. Forest Recovery Execution

SECTION	CONTENT
THE PROBLEM	Forest recovery relies on complex manual procedures, documentation, and individual expertise.
WHY IT MATTERS	Manual recovery processes increase risk, extend downtime, and create uncertainty during major identity incidents.
HOW CAYOSOFT GUARDIAN HELPS	Guardian automates critical forest recovery activities and enables controlled recovery execution with reduced operational risk.
LEARN MORE	Active Directory Forest Recovery: Strategies for 2026

5. Rollback Capability

SECTION	CONTENT
THE PROBLEM	Teams can identify unwanted changes but lack an efficient way to reverse them.
WHY IT MATTERS	Delayed remediation extends operational disruption, increases security exposure, and slows recovery efforts.
HOW CAYOSOFT GUARDIAN HELPS	Guardian enables rapid rollback of accidental, malicious, scripted, automated, or AI-driven changes.
LEARN MORE	7 Best Active Directory Auditing Software Tools Compared

6. Hybrid Visibility

SECTION	CONTENT
THE PROBLEM	Identity evidence is distributed across Active Directory, Entra ID, Microsoft 365, Intune, and other systems.
WHY IT MATTERS	Incident investigations take longer and executives struggle to understand the full scope and business impact of an event.
HOW CAYOSOFT GUARDIAN HELPS	Guardian change monitoring provides a unified identity timeline across the Microsoft hybrid identity stack.
LEARN MORE	Identity attack paths: Why they keep working

CUSTOMER PROOF

“Cayosoft gave us confidence that no matter what happens—cyberattack, misconfiguration, or disaster—we can restore AD quickly and keep the state running.”

Project Lead, State Department of IT

7. AI and Automation Change Control

SECTION	CONTENT
THE PROBLEM	AI agents, scripts, service accounts, and automation can make large-scale identity changes faster than teams can review them.
WHY IT MATTERS	Small mistakes can rapidly become security incidents, operational outages, or compliance issues.
HOW CAYOSOFT GUARDIAN HELPS	Guardian helps organizations identify, investigate, and reverse changes made by both human and nonhuman actors.
LEARN MORE	AI agent action rollback: Cayosoft named by Gartner

8. Privileged Access Recovery

SECTION	CONTENT
THE PROBLEM	Recovery procedures do not clearly address restoration and validation of Tier-0 and privileged access.
WHY IT MATTERS	Recovering administrative access incorrectly can reintroduce attacker persistence or prevent critical recovery activities.
HOW CAYOSOFT GUARDIAN HELPS	Guardian supports secure recovery of privileged identities and validation of administrative access during recovery operations.
LEARN MORE	Identity Recovery and Forest Recovery Protection

9. Recovery Testing Evidence

SECTION	CONTENT
THE PROBLEM	Recovery readiness is assumed based on documentation rather than validated through testing and evidence.
WHY IT MATTERS	Executives and auditors cannot confidently assess recovery capability without recent proof that recovery processes work.
HOW CAYOSOFT GUARDIAN HELPS	Guardian continuously validates recovery readiness and provides evidence that recovery environments and processes remain operational.
LEARN MORE	Forest Recovery in Active Directory: Are You Prepared?

CUSTOMER PROOF

“ We needed to be 100% confident in our security posture. Cayosoft gave us that.

IT Architect, IRS

10. Business Continuity Confidence

SECTION	CONTENT
THE PROBLEM	Identity recovery is viewed as an IT problem rather than a business continuity requirement.
WHY IT MATTERS	Identity outages affect users, applications, productivity, customer operations, and revenue-generating activities across the organization.
HOW CAYOSOFT GUARDIAN HELPS	Guardian helps organizations reduce recovery time, improve operational resilience, and demonstrate recovery readiness to executives and boards.
LEARN MORE	Identity Recovery: Cayosoft Named by Gartner

About Cayosoft Guardian

Cayosoft Guardian helps organizations recover identity faster, reverse unwanted changes, and strengthen operational resilience across Active Directory, Microsoft Entra ID, Microsoft 365, and Intune. It combines identity recovery, rollback, change monitoring, and forest recovery in a single platform to reduce downtime and improve recovery confidence.

With Guardian, organizations can restore identity services in minutes, investigate incidents faster, maintain continuously validated recovery environments, and demonstrate recovery readiness to executives, auditors, and boards.

“ The AD backup and standby forest recovery features are vitally important to our DR procedures.

Gartner Peer Insights Reviewer

CUSTOMER PROOF

“ You know how people ask what keeps you up at night? That doesn't keep me up at night anymore. It just works.

Hussein Alalawi, Senior Security Engineer, AAA

Why Cayosoft

Cayosoft helps organizations achieve identity resilience, strengthen cybersecurity, and recover quickly across the Microsoft hybrid identity stack. Organizations replace fragmented legacy tools with Cayosoft to improve recovery readiness, reduce downtime, and maintain continuous control over identity systems.

Founded by Microsoft platform experts, Cayosoft was built around a simple mission: help organizations secure, manage, monitor, recover, and govern identity from a single operational platform. Cayosoft brings together administration, monitoring, rollback, forest recovery, recovery readiness, delegation, governance, and audit evidence to help organizations operate with greater confidence and less complexity.

BOOK A DEMO

Support resources: support.cayosoft.com | **Product information:** www.cayosoft.com