semperis



WHITE PAPER

Identity-First Security and Crisis Management for Singapore Financial Institutions

Achieving and maintaining cyber resilience in alignment with the Monetary Authority of Singapore Technology Risk Management Guidelines

semperis

Contents

Executive summary 2

MAS TRM Guidelines raise the bar for operational resilience 3

Why identity security is central to MAS Technology Risk Management 4

Where the MAS Guidelines and identity-first security intersect 5

Access management and privileged control 5

Cyber monitoring and incident response 5

Recoverability and disaster recovery testing 5

Governance, exercises, and continuous improvement 5

How Semperis supports Technology Risk Management 6

Lightning Platform 6

Active Directory Forest Recovery (ADFR) 7

Ready1 8

Combined value: From control to resilience 10

What true cyber resilience means for Singapore financial institutions 12

Executive Summary

For financial institutions in Singapore, technology risk is no longer a narrow IT issue. It is a board-level business resilience issue.

The **Monetary Authority of Singapore (MAS) Technology Risk Management Guidelines**[1] make that clear by setting expectations for governance, access control, cyber monitoring, incident response, recoverability, and continuous improvement across the technology estate.

In practice, many of these obligations converge on one foundational layer: *the identity infrastructure*. Active Directory and hybrid identity systems that include Entra ID and Okta underpin authentication, privileged access, system administration, and recovery across core banking, payments, customer portals, and internal operations.

When identity is compromised, attackers do not simply gain access to a directory. They gain a path to the wider enterprise.

That is why an identity-first approach is essential for alignment with MAS Guidelines. With identity at the centre of their cyber strategy, financial institutions reduce risk earlier, detect attacks faster, respond with greater precision, recover critical services more quickly, and demonstrate resilience more credibly to regulators, auditors, and internal stakeholders.

Semperis supports this approach through complementary capabilities:

- **Continuous** identity threat detection, posture monitoring, and rapid response
- **Automated**, malware-free Active Directory recovery
- **Proven** cyber crisis readiness, incident coordination, exercise management, and resilience reporting

Together, these capabilities help financial institutions strengthen the identity layer that is the foundation of many MAS TRM control areas.

More important, they help turn compliance activity into meaningful operational resilience. Instead of treating technology risk as a checklist, institutions can build a more durable capacity for withstanding and recovering from identity-centric attacks.

1 Monetary Authority of Singapore (MAS) Technology Risk Management Guidelines

MAS TRM Guidelines raise the bar for operational resilience

The MAS TRM Guidelines set out principles and best practices for managing technology and cyber risk across Singapore's financial sector. Although the guidance spans governance, architecture, operations, third-party risk, and incident management, the underlying expectation is consistent.

Financial institutions must be able to prevent disruption where possible— and recover quickly when disruption occurs.

That expectation matters because cyber incidents in financial services rarely remain contained. A compromise that begins with a privileged credential, a misconfigured identity trust, or a change to a critical group policy can quickly affect payment systems, customer-facing applications, treasury functions, and internal business operations. The institution is then dealing not just with a security event, but with a business continuity event.

Semperis research shows that financial institutions in general—and enterprise organisations in Singapore in particular—already place great emphasis on preparing for and practicing for cyber incidents. The **State of Enterprise Crisis Readiness**[2] found that Singapore is the only country globally where more than half of organisations include business stakeholders, business continuity teams, and disaster recovery teams in regular cyber crisis tabletop exercises. Even so:

- **53%** of Singapore organisations in the Semperis study still experienced multiple cyber events that were severe enough to halt critical business functions.
- Only **21%** of Singapore financial services organisations are confident that cyber crisis planning efforts can actually protect business resilience.

For that reason, the Guidelines should be read not only as recommended controls. They are guidance on resilience. The MAS expects institutions to know:

- Where their critical dependencies sit
- How those dependencies are monitored
- How incidents are escalated
- How recovery can be executed under pressure

In most financial institutions, identity is the foundation of those critical dependencies.

2 The State of Enterprise Cyber Crisis Readiness | Semperis Reports

Why identity security is central to MAS Technology Risk Management

Active Directory remains the backbone of identity and access management in most banks, insurers, and other financial institutions. It governs authentication, privileged access, policy enforcement, server administration, and trust relationships across large parts of the enterprise. In hybrid environments, it also connects closely with cloud identity systems such as Entra ID.

Attackers understand this. According to Microsoft[3], identity-based attacks rose by 32% in the first half of 2025. Attackers target identity infrastructure because it offers leverage. Once they gain control of privileged identity paths, they can move laterally, escalate privileges, disable defences, manipulate recovery processes, and extend their reach into high-value systems.

> *Cyber risk can no longer be treated as a purely technical issue. This is a core business risk and leadership responsibility. Boards and executives should ensure cyber resilience is in place and works under pressure. It is not enough to have controls. Leaders must be confident those controls will perform during a real incident.*
>
> **Five Eyes Cyber Security Agencies**
> Statement, June 2026

In addition, adoption of AI tools and agents has already transformed the digital attack surface. A Joint Statement from the Five Eyes cyber security agencies[4] spotlights the urgency of recognizing that cyber resilience is an existential issue. Cyber criminals are already using AI to accelerate the pace and efficiency of attacks, and defenders must do the same.

This is why identity-first security is strategically important. Such an approach focuses security investment on the control plane that influences everything else, directly supporting several core Technology Risk Management outcomes:

- Stronger access governance and privileged access control
- Better visibility into suspicious changes and attack activity
- Faster incident containment and cleaner response escalation workflows
- More reliable recovery of critical authentication services
- Stronger audit evidence for testing, remediation, and continuous improvement

In other words, identity-first security does not sit beside the Guidelines. It helps *operationalise* them.

3 Microsoft Digital Defense Report 2025 – Safeguarding Trust in the AI Era

4 How the Five Eyes AI Warning Changes Cyber Recovery and Resilience

Where the MAS Guidelines and identity-first security intersect

Although the Guidelines are broader than any single technology domain, several control areas rely heavily on the integrity, availability, and recoverability of identity systems.

Access management and privileged control

MAS places clear emphasis on disciplined access management and tighter control over privileged accounts. That control is especially important in the identity infrastructure[5], where excessive permissions, stale privileges, shadow admin accounts, and undocumented entitlements create attractive attack paths.

An identity-first approach improves visibility into these issues by establishing continuous assessment of who has elevated access, how that access changes over time, and whether permissions drift away from least-privilege principles.

Cyber monitoring and incident response

MAS also expects financial institutions to maintain effective monitoring and incident response capabilities. In identity-centric attacks, speed matters. Delayed detection can allow attackers to replicate credentials, change privileged groups, alter policies, or establish persistence before traditional monitoring teams understand what is happening.

Monitoring the identity layer directly helps close that gap. It gives security teams earlier visibility into high-risk changes and makes response more precise.

Recoverability and disaster recovery testing

Recoverability is another area where identity often becomes the hidden dependency. If core identity systems are unavailable, business and IT recovery efforts can stall because administrators, applications, and users cannot authenticate. That makes Active Directory recovery a prerequisite for restoring many downstream services.

A resilient institution therefore needs more than backups. It needs a tested, repeatable, cyber-aware recovery capability that can restore the identity plane quickly and safely.[6]

Governance, exercises, and continuous improvement

The MAS Guidelines also reinforce the importance of management oversight, structured exercises, remediation, and lessons learned. These expectations are difficult to meet consistently when response planning is fragmented across spreadsheets, slide decks, and ad hoc runbooks.

An identity-first resilience programme works best when technical controls are paired with structured crisis management. This is the bridge between security operations and regulatory confidence.

5 What Is Identity Attack Surface Management? | Semperis Guides

6 Rapid Identity Recovery: Lessons from Frontline Incident Response

How Semperis supports Technology Risk Management

Semperis helps financial institutions strengthen identity-centric security and control through integrated capabilities across detection, response, recovery, and readiness.

Lightning Platform

The **Semperis Lightning Platform** is designed to speed identity system defence against conventional and agentic threats targeting hybrid Active Directory, Entra ID, and Okta environments.

Its value in the context of MAS Guidelines is not simply that it produces alerts. Lightning connects identity security posture management, attack readiness, and identity threat detection and response in a single console, providing visibility and control that helps institutions manage identity risk as a live operational issue.

Lightning continuously monitors identity infrastructure for suspicious changes, privilege misuse, misconfigurations, and known vulnerabilities. It also supports attack path analysis, privileged account discovery, and risk scoring, helping teams identify weaknesses and prioritise remediation before they are exploited.

From a business perspective, Lightning helps security teams answer three critical questions faster:

- What changed?
- Why does it matter?
- What should we do now?

That speed is important in financial services. For example, if a threat actor attempts an unauthorized privileged group change, teams need immediate visibility and remediation of the action. Lightning provides both through real-time detection, automated rollback of malicious or unauthorised changes, and a unified workflow to enable teams to effectively manage incident response.

The strategic value is broader than containment. By improving visibility into identity vulnerabilities and malicious behaviour, the Lightning Platform helps financial institutions move from reactive incident handling to proactive risk reduction. That is a better fit for the intent of the MAS Guidelines: to both respond well and operate more safely and resiliently over time.

How the Lightning Platform aligns with MAS Technology Risk Management Guidelines

MAS Guideline	How Lightning Helps
Section 9.1 User Access Management	Detects inappropriate access rights grants, dormant accounts, and shadow admin accounts across AD, Entra ID, and Okta. Flags deviations from least-privilege principles.
Section 9.2 Privileged Access Management	Continuously monitors privileged and service accounts for abuse, unusual behaviour, and unauthorised permission changes. Provides automated alerts and rollback.
Section 12.2 Cyber Event Monitoring	Provides 24/7 real-time activity monitoring without relying on Windows event logs, which attackers can evade. Identifies malicious activity associated with advanced attacks.
Section 12.3 Cyber Incident Response	Enables automated detection and rollback of malicious changes as part of the incident response workflow, preventing incidents from escalating into crises.
Section 4.2 Risk Identification	Attack path analysis proactively discovers and automatically maps attack paths to Tier 0 assets and helps identify excessive privileges that attackers can exploit.
Section 11.3 System Security	Continuously validates AD and Entra ID security posture, ensuring the underlying identity systems are secure and trustworthy.
Section 13.1 Vulnerability Assessment	Built-in vulnerability assessment continuously scans for security gaps including Indicators of Exposure and Compromise.

Active Directory Forest Recovery (ADFR)

If Lightning is about posture, detection, and response, ADFR is about ensuring the financial institution can recover the identity plane when prevention is no longer enough.

Active Directory recovery is notoriously complex.[7] Manual recovery is slow, specialised, and difficult to execute consistently during a live cyber event. Worse, rushed recovery efforts can reintroduce malware or configuration issues into the restored environment.

ADFR addresses this challenge through an automated, orchestrated, cyber-first recovery process. It is built specifically to restore Active Directory forests after major cyber incidents, including ransomware events that affect domain controllers and core identity systems.

For Singapore financial institutions, the business case is straightforward. If users, admins, and systems cannot authenticate, other recovery processes slow down or fail altogether. A faster identity recovery process can materially reduce wider business disruption.

7 Top Manual AD Forest Recovery Pitfalls | Semperis Guides

ADFR helps compress recovery time from days or weeks to hours. Crucially, it also supports regular testing of recovery procedures before a real event occurs. That matters not only for resilience, but also for evidence. Institutions must be able to show that recovery plans are practical, tested, and understood.

With ADFR, financial institutions can shift recovery from a fragile expert-led activity to a repeatable institutional capability. That is a meaningful strategic improvement for any organisation seeking to strengthen its resilience posture under MAS scrutiny.

How ADFR aligns with MAS Technology Risk Management Guidelines

MAS Guideline	How ADFR Helps
Section 7.7 Incident Management	Enables rapid restoration of the identity plane as part of cyber incident response, a critical prerequisite for restoring downstream financial applications and services.
Section 8.2 System Recoverability (RTO/RPO)	Dramatically compresses AD recovery time from days or weeks to hours, enabling financial institutions to meet aggressive RTO and RPO commitments for identity infrastructure.
Section 8.3 Disaster Recovery Testing	Enables regular, non-disruptive DR tests of the full AD forest recovery process, supporting MAS requirements for regular DR plan testing.
Section 8.4 System Backup and Recovery	Automates frequent, consistent backups of the AD forest. Backups are stored securely and verified clean before restoration, supporting data integrity and confidentiality.
Section 8.5 Data Centre Resilience	Supports multi-site recovery scenarios, enabling institutions to recover AD in an isolated environment when the primary environment is fully compromised.

Ready1

MAS Guidelines are not only about technical controls. They are also about decision making, accountability, crisis simulation exercises, remediation, and executive oversight. That is where Ready1 adds value.

Ready1 is a cyber crisis readiness platform that helps organisations manage plans, simulation exercises, live response workflows, decision logs, and after-action improvement. The platform gives structure to the operational side of resilience, which is often where institutions struggle to demonstrate maturity.

This matters because a strong technical response can still be undermined by poor orchestration.[8] During a serious identity compromise, teams need clear roles, out-of-band communication, pre-determined escalation points, and documented actions. After the incident or exercise, they need a disciplined way to capture lessons learned, track corrective actions, and report to authorities.

Ready1 helps turn those activities into a structured capability. For executives and regulators, that creates more credible evidence that the institution is not improvising its resilience model. It is managing it.

8 Rethinking Cyber Crisis Management: Why Plans Fail

How Ready1 aligns with MAS Technology Risk Management Guidelines

MAS Guideline	How Ready1 Helps
Section 3.1 Board and Senior Management Oversight	Provides Board-level reporting dashboards showing cyber readiness posture, open action items from exercises, and resolution timelines, enabling informed governance oversight.
Section 3.6 Security Awareness and Training	Supports structured cyber crisis simulation exercises and role-based training scenarios for staff, contractors, and Board members.
Section 7.7 Incident Management	Provides a centralised digital incident management framework covering process workflows, communication plans, role assignments, and stakeholder notifications.
Section 7.8 Problem Management	After-action review workflows capture lessons learned from incidents and exercises, feeding them back into updated response plans to support root cause analysis and recurrence prevention.
Section 8.3 Disaster Recovery Testing	Enables institutions to design, run, and document realistic crisis recovery simulation exercises, including AD recovery, generating audit-ready evidence of testing frequency and outcomes.
Section 12.3 Cyber Incident Response and Management	Provides a structured, tested recovery runbook for AD, reducing dependency on tribal knowledge and helping ensure consistent recovery execution even under crisis conditions.
Section 13.3 Cyber Exercises	Provides a structured platform for planning and executing scenario-based cyber exercises, including tabletop, crisis simulation, and adversarial scenarios, with documented outcomes aligned to MAS expectations.
Section 13.6 Remediation Management	Tracks remediation actions identified in cyber exercises and assessments, including severity classification, ownership, target dates, and signoff, providing a full audit trail for review.

Combined value: From control to resilience

The strongest outcomes are possible when the Lightning Platform, ADFR, and Ready1 are used together.

Individually, each element strengthens a different part of the MAS Guidelines. Together, they create a more complete identity resilience operating model.

This combination supports a broader shift in posture:

- From static compliance documentation to live operational readiness
- From siloed tools to connected resilience workflows
- From delayed discovery to earlier detection and prioritized response
- From untested recovery assumptions to repeatable recovery execution
- From anecdotal preparedness to audit-ready evidence

> *Cyber incidents don't wait for organizations to be ready—they strike when you're least prepared. In a crisis, you don't rise to the occasion. You fall to your level of preparedness.*
>
> **Marty Momdjian**
> Global Field CTO, Semperis

That is the strategic point. Alignment with MAS Guidelines requires more than mapping products to guidance. It's about enabling financial institutions to operate with greater confidence in the face of escalating identity-centric risk.

How Semperis supports institutions through the full cyber lifecycle

Technology Risk Management Phase	Semperis Solutions	Capabilities
Proactive Risk Identification	Lightning + Ready1	Lightning provides continuous threat and vulnerability assessment and visibility into identity security posture; Ready1 enables structured cyber exercise planning to identify gaps in crisis response before attackers do.
Continuous Monitoring and Detection	Lightning	Lightning provides 24/7 real-time monitoring of identity (AD, Entra ID, and Okta) infrastructure for multi-forest and multi-tenant environments, provides a visual dashboard to track security posture scores across the hybrid environment, continuously conducts identity inventories, and scans for 250+ indicators of exposure continuously updated by an expert threat research team.
Incident Response	Lightning + Ready1	Lightning provides automated rollback of risky and malicious changes; Ready1 centralises and unifies all aspects of cyber crisis planning and incident response.
Disaster Recovery	ADFR + Ready1	ADFR automates full, malware-free AD forest recovery, including relevant dependencies; with up-to-date, tested playbooks and a secure out-of-band platform, Ready1 ensures seamless crisis response through preparation, collaboration, and enterprise-wide communications.
Regulatory Reporting	Lightning + ADFR + Ready1	Lightning provides security posture dashboards and exportable reports to support audit and remediation tracking; ADFR enables post-breach forensics to identify persistence and recover AD to a trusted state; Ready1 automatically generates exercise reports and remediation tracking to demonstrate MAS Guidelines alignment and resilience progress.

What true cyber resilience means for Singapore financial institutions

The MAS Technology Risk Management Guidelines set a clear expectation for financial institutions in Singapore: technology risk must be managed as an enterprise resilience issue. Access governance, monitoring, response, recovery, and continuous improvement are all part of that mandate.

For CISOs, security leaders, and compliance teams, the immediate takeaway is clear: identity should be treated as a Tier 0 resilience domain, not a background service.

Institutions that continue to view Active Directory and hybrid identity primarily as "infrastructure components" risk underinvesting in one of the most important layers in their control environment.

Institutions that take an identity-first view are better positioned to:

- Reduce the likelihood of privilege abuse and identity-driven lateral movement
- Detect critical attacks earlier in the kill chain
- Restore authentication services faster after major incidents
- Improve the quality and repeatability of cyber exercises
- Produce clearer evidence of operational resilience to internal and external stakeholders

This does not mean identity tools alone create compliance. MAS TRM requires governance, policy, process discipline, and a broader control environment. But it does mean that identity resilience can act as a force multiplier across many of those obligations.

Semperis supports these outcomes through an identity-first approach that spans prevention-oriented visibility, real-time response, cyber-first recovery, and crisis readiness. The Lightning Platform, ADFR, and Ready1 do more than simply help institutions respond to individual incidents. Together, they help create a stronger and more defensible organisation.

For Singapore financial institutions, that is the real opportunity: to not just meet the Guidelines but also build a more resilient identity foundation for the business.