USE CASE | FINANCIAL SERVICES

IAM Resilience for Financial Services

Protect. Recover. Remain Operational.

Executive Summary

In financial services, identity systems are Tier-0 operational infrastructure. Identity state — encompassing users, groups, applications, policies, and their dependencies — is the foundation that authenticates customers, authorizes transactions, enables trading platforms, and governs workforce access to critical systems.

Identity providers such as Okta, Entra ID, and Ping are responsible for platform availability. They are not responsible for the integrity, configuration, or recoverability of your IAM tenant. That responsibility belongs to you.

When IAM fails — due to misconfiguration, destructive change, ransomware, or operator error — operations stop immediately. High availability is not enough. Financial institutions must be able to recover identity state quickly, validate recovery readiness continuously, investigate incidents with full historical context, and prove resilience to regulators.

Acsense delivers IAM Resilience: the ability to recover IAM environments within defined RTO/RPO targets, continuously validate recovery readiness, investigate identity incidents over time, and generate audit-ready evidence for regulators and auditors.

$6.08M
Average breach cost
Financial industry — among the highest of any sector (IBM)

94%
Backups targeted
Of ransomware victims report attackers attempted to compromise backups (Sophos)

$1.1B+
SEC penalties
16 Wall Street firms penalized for recordkeeping and control failures (SEC, Sept. 2022) — operational gaps carry real financial consequences

The Financial Services Challenge

01 IAM Outages Have Immediate Business Impact

Identity is not a supporting control — it is a single operational dependency for every downstream system. A failed IAM change, destructive attack, or misconfiguration can:

- Lock out customers and employees from critical applications and services
- Halt payments, trading, and customer servicing workflows
- Break cascading access dependencies across SaaS, cloud, and on-premises systems
- Trigger SLA breaches, regulatory escalation, and reputational damage

02 IDPs Ensure Availability — Not Your Identity Recoverability

This is the shared responsibility gap financial institutions consistently underestimate. Okta, Entra ID, and Ping guarantee their platform is operational. They do not:

- Restore your identity configurations after a destructive change
- Recover applications, groups, policies, and their relationships in the correct order
- Provide tested, dependency-aware recovery within a defined RTO/RPO
- Generate audit-ready evidence that your identity state is recoverable

> *Backup alone does not ensure operational continuity. Snapshots without dependency awareness, recovery validation, or proof do not guarantee working authentication.*

03 Identity State Complexity Makes Recovery Fragile

IAM state is not a flat file. Identity environments span users, groups, applications, policies, entitlements, and dependencies. Most recovery approaches fail because:

- Flat-file restores break relationships between users, groups, apps, and policies
- Recovery relies on manual scripts, spreadsheets, and tribal knowledge
- Disaster recovery plans are documented but rarely validated against actual identity state
- Change velocity — from automation, M&A, and app onboarding — introduces continuous configuration drift

04 AI Agents and Non-Human Identities Expand Blast Radius

Identity now encompasses more than human users. Service accounts, automation pipelines, and AI agents have proliferated across modern financial services environments. These non-human identities:

- Often carry elevated privileges with limited visibility and audit coverage
- Create additional blast radius when identity systems fail or are compromised
- Are increasingly scrutinized by regulators who require full audit trails and provable control

05 Regulators Require Evidence, Not Assertions

Financial services organizations operate under one of the most demanding regulatory environments for identity and access controls. Frameworks including DORA, NIS2, PCI DSS, SOX, GLBA, FFIEC, NIST CSF, NIST SP 800-53, ISO 27001, and CPS 230 now explicitly require:

- Defined and tested recovery objectives (RTO/RPO) for critical operational systems
- Regular, validated disaster recovery testing — not assumed readiness
- Audit-ready evidence of control effectiveness and recoverability

Key frameworks and what they require of IAM:

- **DORA (EU):** Mandates ICT resilience testing, incident reporting, and recovery capability for financial entities operating in the EU
- **NIS2 (EU):** Requires risk management measures and business continuity controls, including for identity and access systems
- **FFIEC:** US banking regulators explicitly address identity and access management as a core control domain requiring evidence of effectiveness
- **GLBA:** Requires financial institutions to implement safeguards protecting customer data, including access controls and audit trails
- **PCI DSS:** Mandates strict access control, least privilege, and audit logging for systems handling cardholder data
- **SOX:** Requires demonstrable controls over systems that affect financial reporting, including access governance and change management
- **NIST CSF & SP 800-53**: Widely adopted baseline for US financial institutions; SP 800-53 includes detailed controls for identity management, recovery, and audit
- **ISO 27001:** International standard requiring documented access control policies, change management, and business continuity for information security
- **CPS 230 (Australia):** APRA's operational risk standard requires financial institutions to demonstrate resilience and recoverability of critical systems

> *IAM is now part of operational resilience and regulatory accountability. Recovery readiness must be provable — not assumed.*

The Acsense IAM Resilience Stack

Acsense treats IAM as critical operational infrastructure that must be recoverable, testable, and auditable. Most vendors address only one layer of this problem. Acsense delivers all four.

LAYER 1 **Identity State Foundation** *Backup vendors stop here*	• Continuous capture of authoritative identity state — not just exported objects • Immutable, time-sequenced history of identity changes • Known-good recovery points across tenants
LAYER 2 **Identity State Observability** *IVIP and visibility vendors stop here*	• Time-based identity investigation (Time Machine) — trace exactly what changed and when • Full identity timelines, state transitions, and dependency context • Blast-radius analysis to understand incident scope before recovery
LAYER 3 **Resilience Operations** *Uniquely Acsense*	• Dependency-aware recovery — restoring working authentication flows, not just data • Tenant-level restore and rebuild within defined RTO/RPO targets • Automated IAM disaster recovery drills as continuous validation — not periodic exercises • Measured and enforced RTO/RPO aligned to financial services requirements
LAYER 4 **Auditability & Proof** *Where regulated buyers lean in hardest*	• Recovery evidence and integrity checks — proof, not promises • Time-based entitlement evidence for non-human identity audit trails • Regulatory reporting aligned to DORA, NIS2, PCI DSS, SOX, GLBA, FFIEC, NIST CSF, NIST SP 800-53, ISO 27001, and CPS 230 • Proof of recovery readiness defensible to boards, regulators, and auditors

Core Outcomes for Financial Institutions

Business KPI	Why It Matters	Acsense Impact
IAM Recovery Time (RTO)	Every minute of identity downtime halts transactions, trading, and servicing	Restore full IAM environments within minutes, aligned to defined SLAs
Recovery Readiness	Untested recovery plans fail under pressure — at exactly the moment they are needed	Continuous automated DR drills validate readiness before an incident occurs
Regulatory & Audit Readiness	DORA, NIS2, PCI DSS, and SOX require evidence of control — not assertions	On-demand reports with tested recovery evidence ready for regulatory review
Incident Investigation	Understanding exactly what changed, when, and why is prerequisite to safe recovery	Full historical identity state supports forensics, root-cause analysis, and compliance
Operational Efficiency	Manual IAM recovery drains lean teams and increases error risk during incidents	Automated, guided recovery replaces scripts and tribal knowledge

Why This Matters Now

Attackers, regulators, and auditors have converged on identity as the primary operational risk surface in financial services:

- **Attackers target recoverability directly.** 94% of ransomware victims report that attackers attempted to compromise their backups (Sophos). Backup alone is not recovery.
- **Regulators are enforcing controls.** The SEC, DORA, NIS2, and regional banking authorities are moving from guidance to enforcement. Operational control gaps result in real financial penalties.
- **AI agents and non-human identities have expanded the attack and audit surface.** Identity now includes automation and AI agents — and regulators expect full audit trails across all of them.
- **Identity failures are no longer hypothetical.** Misconfigurations, destructive changes, and supply chain attacks on identity systems are occurring at scale.

> *IAM Resilience is no longer optional — it is a requirement for operational continuity and regulatory compliance in financial services.*

About Acsense

Acsense is the IAM Resilience Platform for modern enterprises. We enable organizations to protect and recover their IAM tenant and identity configuration state within defined RTO/RPO targets. Acsense provides continuous visibility into identity configurations and changes, validates recovery readiness, enables full historical investigation of identity incidents, and delivers auditable proof of control across Okta, Entra ID, and Ping — addressing the customer's responsibility for identity continuity beyond the identity provider's scope.

Learn more at **www.acsense.com**