RSA

SOLUTION BRIEF

Secure, Compliant, and Continuous Identity Governance for Financial Services

From compliance to continuous control: how RSA supports financial services

Financial services organizations operate in one of the most targeted threat environments in the world. Identity-based attacks remain a primary entry point for breaches and fraud, with **72%** of financial institutions experiencing an identity-related breach over a three-year period. As environments grow more complex, with employees, contractors, third parties, and non-human identities all requiring access across on-premises, cloud, and hybrid systems, traditional governance models can no longer keep pace.

RSA® Governance & Lifecycle helps financial institutions and other financial services organizations move beyond periodic compliance activities to a continuous, defensible identity governance posture. With AI-driven risk insights, automated lifecycle management, and real-time policy enforcement, organizations can reduce identity risk, close the gap between documented policy and actual access, and meet regulatory obligations before they become audit findings.

Excessive access and insider risk

Financial services organizations rely on a complex mix of employees, contractors, and third-party partners across lines of business and systems. Managing access manually leads to permission sprawl, excessive entitlements, and orphaned accounts that persist long after they should. When access issues go unnoticed for months, the cost is not just financial. It is operational disruption, regulatory exposure, and loss of confidence.

How RSA helps:

- Enforces least-privilege access and role-based access controls (RBAC) to limit exposure across all user types
- Automates onboarding, offboarding, and access changes to ensure users have the right access at the right time and nothing more
- Applies AI-driven analytics to continuously evaluate access and surface anomalies before they become incidents
- Provides the continuous visibility into identities, roles, and entitlements needed to understand and improve identity security posture across on-premises and cloud environments, including non-human identities

Regulatory compliance and audit readiness

Financial institutions and other financial services providers face constant scrutiny from regulators and auditors under frameworks such as SOX, 23 NYCRR Part 500, PCI-DSS, and other requirements which require strong identity controls, auditability, and governance. Periodic reviews and manual processes create a gap between documented policy and what systems are actually doing, and in a breach scenario, that gap is where liability lives.

Built for finance

Trusted by the world's most secure financial institutions, including:

- **70% of Fortune 1,000 financial services organizations**
- **50% of Fortune 100 financial services organizations**

Key regulations addressed

- **FFIEC Authentication Guidance**
- **23 NYCRR Part 500**
- **SOX / GLBA / PCI-DSS**

Deployment models

On-premises

Cloud

Hybrid (cloud and on-premises)

What RSA Governance Lifecycle governs:

- Human identities
- Non-human identities
- Privileged and high-risk entitlements

How RSA helps:

- Automates access reviews, certifications, and segregation of duties (SoD) controls to reduce compliance gaps and reviewer fatigue
- Provides continuous, tamper-evident audit trails that demonstrate policy enforcement
- Generates customizable reports aligned to SOX, 23 NYCRR 500, PCI-DSS, as well as other regulatory frameworks and internal policy requirements
- Helps institutions maintain compliance by enforcing identity policies consistently across all connected systems whether on-premises or in the cloud

Privileged access sprawl and toxic combinations

Over time, users accumulate high-risk entitlements or conflicting permissions, such as the ability to both create and approve transactions, that create fraud risk and audit exposure.

These toxic combinations frequently go undetected until they become a material audit finding or a loss event. Standard review campaigns, relying on managers certifying access they lack the context to evaluate, are not reliable enough to catch them.

How RSA helps:

- Uses AI-driven insights to identify high-risk entitlement combinations and anomalous access patterns that periodic reviews miss
- Detects and enforces SoD controls across a broad range of on-premises and SaaS applications, remediating violations before they become audit findings or fraud risks
- Provides contextual AI guidance during access reviews, helping reviewers focus on what matters most and reducing reliance on rubber-stamp approvals
- Tracks all access changes with detailed audit logs so investigators and examiners have a precise, documented record of who had access to what and when

Built for financial organizations that can't afford to get identity wrong

For more than 40 years, RSA has helped financial services organizations and other security-first organizations protect critical systems, safeguard sensitive data, and support mission-critical operations.

RSA Governance & Lifecycle delivers AI-powered insights, automated lifecycle management, and continuous compliance controls that help reduce identity risk, meet regulatory obligations, and strengthen operational resilience.

To learn more about how RSA secures identity for financial institutions worldwide, visit **RSA.com/solutions/financial-services**.

About RSA

RSA is the identity standard for government agencies, finance, and high-assurance organizations. RSA provides the identity intelligence, authentication, access, governance, and lifecycle capabilities needed to prevent threats, secure access, maintain operations, and surpass compliance. More than 9,000 security-first organizations trust RSA to manage more than 60 million identities across on-premises, hybrid, and multi-cloud environments. For additional information, visit our website to **contact sales**, **find a partner**, or **learn more** about RSA.