DASHLANE

Credential Compliance for Financial Services CISOs

What examiners expect, where organizations fall short, and how security leaders can close the gap in credential security

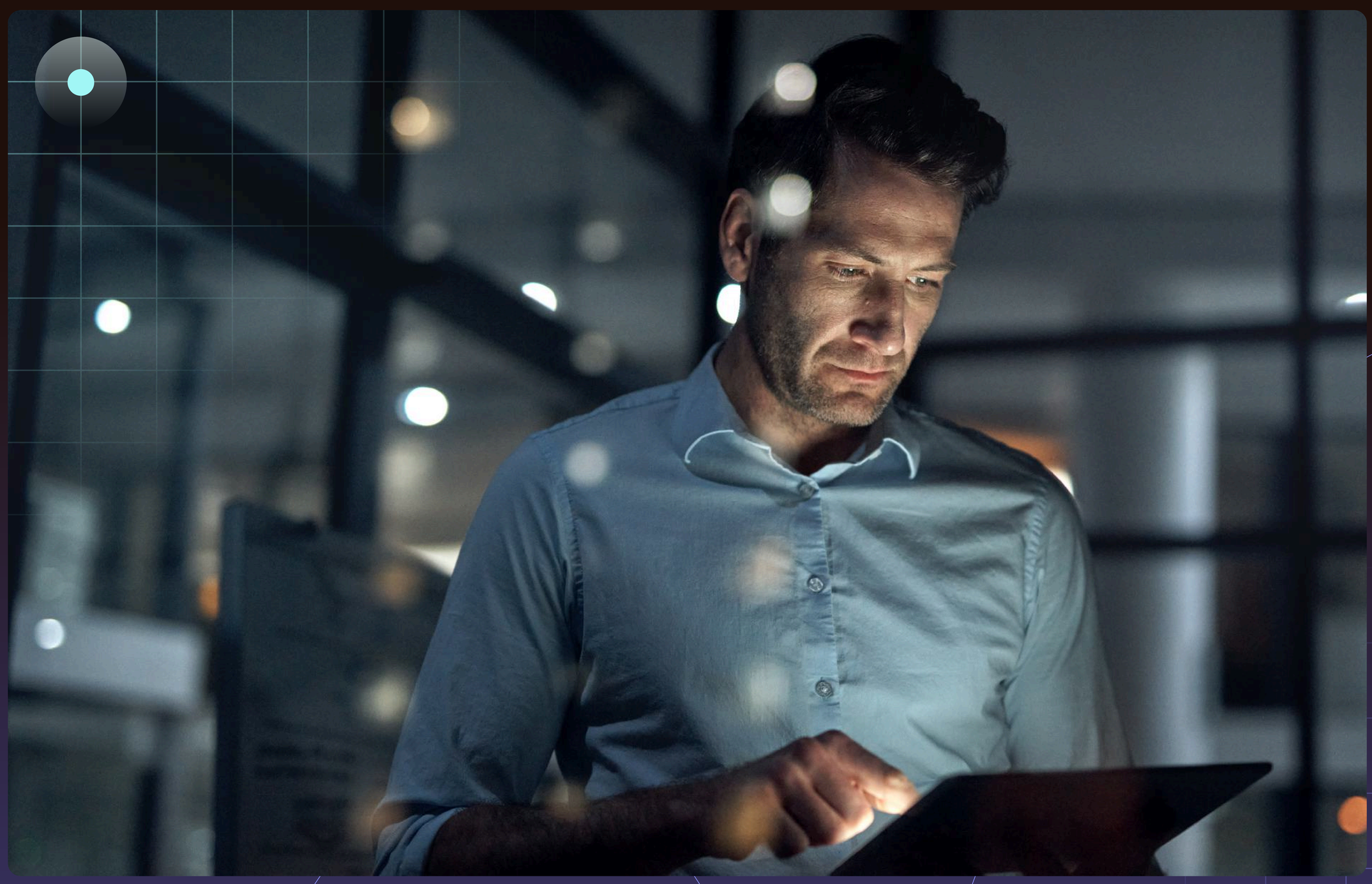

Table of contents

Executive Summary

Financial institutions have invested heavily in credential security like password vaults and single sign-on (SSO), but these tools govern only the credentials they can see. Daily authentication activity across legacy systems, unmanaged applications, shared credentials, and AI agents remain completely outside security teams' oversight.

At the same time, regulators are raising the bar for evidentiary standards. The disconnect between what organizations report and what they can actually prove during an audit is becoming a material compliance risk.

This guide explains to senior security leaders why this disconnect exists, the impact on financial services organizations, and what it takes in practice to achieve continuous, workforce-wide credential protection.

The credential gaps your tools aren’t showing you

Finance security leaders who have deployed a password manager, SSO, and multi-factor authentication (MFA) often believe their credential posture is covered. But these tools don’t extend consistently to all employee logins, leaving organizations with both coverage and evidence gaps.

SSO excludes a substantial portion of credentials from consistent policy enforcement. IT leaders estimate 37% of corporate applications fall outside SSO.[1]

Many legacy banking systems, compliance tools, partner portals, and shadow SaaS applications operate outside centralized authentication, with credentials that security teams can’t consistently monitor or control.

Traditional password managers protect only what employees store in them, and adoption rarely reaches full coverage. Credentials outside the vault are absent from password health reports, not subject to policy enforcement, and excluded from audit records. These logins represent a significant fraction of daily credential use across the workforce. And regulators have noticed.

> The financial sector has the second-highest data breach cost globally, averaging $5.6 million, according to IBM.[2] In the U.S., financial services was the most breached industry in 2025, with 739 confirmed data compromises.[3]

The proof examiners now require

Regulators have continued to raise their expectations for credential controls. Across the major frameworks governing financial institutions, the direction is consistent: Documentation of policy is no longer enough.

However, traditional password management, built around vault adoption and SSO coverage, wasn't designed to prove control effectiveness across all systems and users. Point-in-time snapshots go stale as credentials change, employees turn over, and new apps appear daily.

Examiners want ongoing, verifiable proof that controls work across the full workforce.

Key mandates show a shift toward proving controls in operation, such as enforcing password strength, applying MFA to non-SSO apps, and providing evidence of remediation workflows.

(See Appendix A for requirements, including PCI DSS v. 4.0, GLBA Safeguards Rule, SOX, SEC cybersecurity disclosure rules, and DORA.)

Organizations with traditional password management don't satisfy these requirements. They have critical gaps in their approach, especially around visibility into how employees use their credentials in the browser.

9 in 10 financial services organizations say their compliance landscape has become more complex over the last three years.[4]

Most teams also rely on manual processes, and providing continuous, up-to-date documentation requires automation.

While 88% of surveyed security and compliance professionals feel confident they would pass a surprise audit, nearly half spend more than 10 hours each month preparing evidence.[5]

Manual workflows add to the preparation burden and still leave issues that examiners identify.

> "The regulatory direction of travel is clear: Supervisors expect demonstrable governance, not theoretical frameworks.[6]
>
> **Gavin St John-Heath**
> Global Compliance Institute, Nov 2025

Mapping the credential surface

A typical financial institution's credential surface spans several distinct zones, each with a different level of governance:

- **Managed applications** protected by SSO, where credentials are governed, monitored, and auditable
- **Unmanaged applications** outside SSO, such as legacy core banking systems, compliance tools, partner portals, and shadow SaaS that employees adopt without IT approval
- **Shared credentials** used across teams or offshore operations, often distributed through email or chat and without an audit trail
- **Privileged accounts**, governed by privileged access management (PAM) but frequently having excessive permissions, irregular rotation, and limited oversight after initial provisioning
- **AI agents** that authenticate to systems on behalf of employees, creating machine-to-application access paths that traditional credential tools can’t govern

Shadow IT and, increasingly, shadow AI complicate oversight as employees adopt tools outside security teams’ visibility. Agentic AI introduces another layer of exposure. Agents authenticate to systems on behalf of employees, creating access pathways that are difficult to attribute, monitor, and document.

Financial services regulators recognize the growing AI risk and are starting to flag areas of concern. Yet only 13% of organizations feel highly prepared for regulatory scrutiny of AI agents, which typical credential governance programs don’t address.[7]

Does your credential coverage match your compliance exposure?

- **What percent of the applications used daily by your employees fall outside SSO?** How confident are you in that estimate? Most IT leaders significantly underestimate this figure.
- **Do you have visibility into how shared credentials are distributed and used across teams?** Without centralized control, shared credentials may outlive the employees and workflows they were intended for.
- **Can you provide credential hygiene evidence for every employee, not just those enrolled in your password manager?** If not, your compliance reporting contains a gap that examiners will identify.
- **Do you have a governance framework for AI agents authenticating to systems?** Without a delegation model, agents inherit employee access and become indistinguishable from human users, making it impossible to create the audit trail regulators increasingly expect.

From reactive to demonstrable: Closing the evidence gap

Credential security programs typically have four blind spots: Access, adoption, visibility, and response. Regulators are paying close attention to all of them, and they want three types of proof:

- **Hygiene:** Password strength enforcement and MFA status across the workforce
- **Protection:** Phishing interception and real-time alerting at the point of credential use
- **Remediation:** Recorded workflows showing how credential risks were identified and resolved

Typically, teams can demonstrate hygiene and phishing protection, but proving remediation remains challenging.

A missing layer in credential security programs is browser-native visibility. Whether they're stored in a vault or not, most credentials are used in the browser, where network and endpoint tools can't consistently observe their use. With browser-native visibility, teams can continuously monitor credential activity in real time, across all logins and employees, including those outside traditional control points.

Point-in-time audits provide snapshots that are immediately outdated, while continuous, workforce-wide credential monitoring delivers up-to-date data. Automating this process allows teams to address risks proactively rather than reacting to audit findings.

This practical maturity model helps security teams benchmark what's missing from their framework so they can advance it:

Stage	What's covered	Reporting
Traditional password management	Enrolled users only	Static password health reports for a subset of the workforce; insufficient for audit
Browser-extended	All employees, all logins	Continuous monitoring, real-time alerts regardless of vault adoption
Fully demonstrable	Full workforce + AI agents	Audit-ready hygiene, protection, and remediation evidence across all credential types

Making the case before the next audit finding

For many security leaders, the conversation starts with an internal audit finding, which may include unmanaged credentials, MFA gaps in non-SSO systems, or shared accounts with no audit trail. To secure board investment, CISOs must reframe these credential risks in financial and strategic terms.

Boards respond to framing that highlights risk magnitude, regulatory exposure, and financial impact. In financial services, that impact is concrete: Supervisory findings can result in fines, remediation mandates, independent reviews, and follow-up examinations.

To build a compelling narrative, consider these questions to define the exposure scope before presenting to the board:

- How much visibility do you have into credentials used outside your password manager?
- Can you demonstrate MFA enrollment status for non-SSO applications across the workforce?
- How long would it take to produce a complete credential health report for every employee if an examiner asked for it today?

Addressing these challenges requires extending credential visibility and control to where authentication actually occurs across the workforce.

Dashlane Omnix™ is designed to close the credential coverage gap by protecting every employee login in the browser, not just those in the vault.

Omnix provides continuous monitoring, real-time alerts, and audit-ready reporting from day one. Financial services organizations can demonstrate compliance organization-wide without needing full vault adoption first.

> The disconnect between security leaders' and directors' priorities is growing. Boardroom alignment with CISOs has dropped from 84% to 64% year-over-year, even as business valuation following a cyberattack now ranks as directors' top concern.[8]

Build a more defensible compliance posture

Regulators have made their expectations clear: continuous, documented evidence of credential controls for the entire workforce. Internal audits are increasingly surfacing the gaps.

However, most security teams can only provide partial evidence covering enrolled vault users and SSO-governed applications.

Meeting these standards requires a new approach to credential security. Rather than assuming coverage based on deployed tools, the goal is to actively demonstrate it for all employees, applications, and logins.

Leading security teams are already making this shift, building a credential compliance posture that withstands scrutiny.

Get a credential coverage assessment to understand where your gaps are.
Request your assessment

See how Omnix delivers audit-ready credential reporting across your full workforce from day one.
Learn more

Appendix A: Regulatory reference for credential control requirements

Framework	Scope	Credential-specific requirements	Enforcement
PCI DSS v4.0	Any organization storing, processing, or transmitting cardholder data	Minimum 12-character passwords (Req. 8.3.6); MFA required for all access to the cardholder data environment (Req. 8.4.2); prohibition on hard-coded passwords for application and system accounts (Req. 8.6.2); user accounts inactive for 90 days must be removed or disabled (Req. 8.2.6); password rotation requirements based on account type and authentication method (Reqs. 8.3.9, 8.6.3); daily automated log reviews for critical systems (Req. 10.4.1.1) and periodic, risk-based for others (Req. 10.4.2)	Enforced by payment card brands (Visa, Mastercard, Amex, Discover, JCB) through acquiring banks; non-compliance can result in fines of $5,000-$100,000 per month, increased transaction fees, or loss of card processing rights
GLBA Safeguards Rule	Non-bank financial institutions under FTC jurisdiction; banking institutions under federal banking agency jurisdiction	MFA required for any individual accessing any information system containing customer information (or equivalent approved control); access controls limiting access to authorized users and only necessary customer information (principle of least privilege); periodic review of access and authentication controls; written incident response plan for unauthorized access to customer information; data and systems inventory covering all systems where customer information is collected, stored, or transmitted; breach notification to FTC within 30 days for incidents affecting 500+ consumers	FTC; penalties up to $100,000 per violation for institutions; officers and directors up to $10,000 per violation and up to five years imprisonment for willful violations
SOX Section 404	Publicly traded U.S. companies and their subsidiaries	IT General Controls (ITGCs) require that only authorized personnel access systems impacting financial reporting, with documented audit trails, periodic access recertification, and segregation of duties. Password controls and credential governance are assessed as part of ITGC reviews; MFA is treated as a baseline expectation by external auditors and the Public Company Accounting Oversight Board (PCAOB), even though not explicitly mandated in the statute.	SEC and PCAOB; material weaknesses must be publicly disclosed; penalties include restatement of financials, SEC enforcement, and personal liability for executives (up to $5M fines, 20 years imprisonment for willful violations)
SEC Cybersecurity Disclosure Rules	Publicly traded U.S. companies	Material cybersecurity incidents must be disclosed within four business days of determination of materiality (Form 8-K); annual disclosure of cybersecurity risk management processes, governance, and strategy in Form 10-K filings, including description of processes for assessing, identifying, and managing material cybersecurity risks; board oversight of cybersecurity risk must be documented	SEC; material cybersecurity incidents must be disclosed within four business days of determining materiality; failure to disclose or misleading disclosures can result in SEC enforcement actions, financial penalties, and reputational consequences
DORA	All EU financial entities including banks, insurance companies, investment firms, payment institutions, and crypto-asset service providers; applies to non-EU ICT service providers serving EU financial entities. Exemptions apply to small insurance and reinsurance undertakings exempt from Solvency II, insurance intermediaries that are microenterprises or SMEs, and certain other small entities; a simplified framework applies to microenterprises.	Article 9 makes credential security a binding financial risk control: Strong authentication required for all systems, with phishing-resistant MFA for critical access; access rights must be granted on a need-to-know basis with documented justification; privileged access must be specifically controlled and monitored; credential and access rights must be reviewed at minimum annually and revoked immediately upon role change or departure; complete audit trails required for all access to critical systems; ICT third-party providers must demonstrate equivalent credential controls	European Supervisory Authorities (EBA, EIOPA, ESMA) and national competent authorities; fines up to 2% of total annual worldwide turnover or €10 million (whichever is higher) for financial entities; individual senior managers up to €1 million; critical ICT third-party providers up to €5 million or 1% average daily turnover

Appendix B: Credential coverage self-assessment

Use this checklist to assess your organization's credential coverage. Share it internally with IT, security, and compliance stakeholders.

SSO and applications

- [ ] Do you have a complete and current inventory of all applications employees access for work?
- [ ] Do you know what percentage of those applications fall outside SSO?
- [ ] Can you demonstrate that non-SSO applications have alternative credential controls in place?
- [ ] Do you have visibility into shadow SaaS applications adopted without IT approval?

Vault and password management

- [ ] Do you know what percentage of your workforce has enrolled in your password manager?
- [ ] Can you produce credential hygiene evidence, such as password strength and compromised credential status, for employees outside the vault?
- [ ] Can you demonstrate MFA enrollment status for non-SSO applications for the full workforce?
- [ ] Can you produce a complete credential health report for every employee within 24 hours if an examiner requested it today?

Shared and privileged credentials

- [ ] Do you have a documented process for how shared credentials are distributed and rotated?
- [ ] Can you confirm that shared credentials are revoked promptly when employees leave or change roles?
- [ ] Are privileged accounts reviewed regularly for excessive permissions and inactive access?

AI agent access

- [ ] Do you have a complete inventory of AI agents operating in your environment?
- [ ] Do you have a governance framework defining how credentials are delegated to AI agents?

References

1. Dashlane, "New Data Shows How Shadow IT and Burnt-Out IT Teams Impact Business Security," April 2025.

2. IBM, “Cost of a Data Breach Report,” 2025.

3. Identity Theft Resource Center, “2025 Annual Data Breach Report,” February 2026.

4. PwC, “PWC’s Global Compliance Survey: Accelerating success in financial services,” 2025.

5. StrongDM, “The State of Compliance in Financial Institutions,” August 2025.

6. Global Compliance Institute, “Financial Services Compliance in 2025: Lessons Learned, Systemic Shifts, and the Road Ahead for 2026,” November 2025.

7. Cloud Security Alliance, “Enterprise AI Security Starts with AI Agents,” April 2026.

8. Proofpoint, “Proofpoint’s 2025 Voice of the CISO Report Reveals Heightened AI Risk, Record CISO Burnout, and the Persistent People Problem in Cybersecurity,” August 2025.