

Sponsored content | White paper

5 identity security questions CISOs must be ready to answer

Use this guide to help determine your organization's audit readiness and identify identity security gaps to help reduce executive risk.



CSO

Sponsored by



The new standard for executive accountability

For today's C-suite, reducing risk requires far more than passing the next annual audit; it is about implementing the controls that help mitigate organizational and personal risks in near real time.

As enterprise ecosystems rapidly expand to include not just employees and contractors, but also machine identities and autonomous AI agents, legacy identity governance tools can no longer keep pace. Security leaders are increasingly expected to demonstrate ongoing, real-time oversight through a modern identity security program, rather than relying on the dangerous blind spots of point-in-time reviews.

Foundry [research identifies identity security](#) as one of the top cybersecurity priorities for 2026, reflecting the growing complexity of managing both human and non-human identities. At the same time, streamlining compliance and privacy efforts remains a top priority for CISOs.

The following questions can help security leaders assess their organizations' readiness for continuous identity governance and identify potential gaps before they become security or compliance issues.



❑ Can we centrally identify every identity operating across our environment?

Ask yourself:

- Can we continuously discover and inventory human, third-party, machine, service, and AI identities?
- Do we maintain a centralized, current system of record across the identity ecosystem?
- Can we identify unknown, orphaned, or unmanaged identities before they become security risks?

Why visibility works: After separating from its parent company, [Endeavour Group](#) consolidated multiple HR systems into a single source of truth for more than 30,000 workforce identities. The result: consistent visibility across a complex, multi-brand environment while simplifying identity management for a highly seasonal workforce. The unified identity foundation also enabled more consistent governance as employees joined, changed roles, and moved across brands.

❑ Can we demonstrate who — or what — has access to critical systems at any given time?

Ask yourself:

- Can we continuously monitor identity relationships, entitlements, and privileged access?
- Do we validate that access remains appropriate as users, systems, and business needs change?
- Are least-privilege principles consistently enforced across all identity types?

Why a unified identity approach works: A global digital infrastructure company replaced fragmented identity processes with centralized governance, increasing identity visibility tenfold across cloud, SaaS, and on-premises environments. Security teams gained a unified view of who has access to critical resources, improving both security and operational oversight. The organization also eliminated manual access processes, helping ensure that permissions remained aligned with business needs as users joined, changed roles, or left the company.

❑ Is our approach to access static, or is it truly adaptive?

Ask yourself:

- Is our identity lifecycle management fully automated from day-one provisioning through last-day revocation?
- Do we leverage adaptive identity security that uses AI and machine learning to help dynamically validate and adjust access based on changing user contexts and risk behaviors?
- Have we eliminated the manual provisioning, deprovisioning, and policy enforcement activities that cause compliance drift?

How an adaptive approach supports

continuous governance: TMF Group

automated identity lifecycle management across its global operations, replacing manual processes with standardized workflows. The organization improved consistency while ensuring access remained aligned with changing roles and business requirements. Centralized governance also gives security teams greater visibility into identities across its global environment, helping reduce compliance risk as the company continues to grow.

❑ Can we quickly produce the evidence auditors and regulators require?

Ask yourself:

- Can we maintain audit-ready records of identity ownership, approvals, and policy enforcement?
- Can we demonstrate governance through continuous evidence rather than manual documentation?
- How quickly can we respond to auditor requests?

Why an automated identity approach

works: A global technology company

simplified audit preparation by automatically logging governance activities and access decisions. Auditors can now review consistent, system-generated records rather than relying on manually assembled documentation, reducing the time and effort required to demonstrate compliance.

❑ Do we have the unified identity security foundation needed to adapt to evolving regulations?

Ask yourself:

- Can our policies dynamically adapt alongside strict new mandates and emerging threat vectors like AI agents?
- Can we proactively detect and remediate access anomalies before they become formal compliance findings?
- Are our security, risk, and compliance efforts operating from a single, unified system of record for all identities?

Why a centralized identity solution works:

UniSuper centralized identity information from multiple disconnected sources, creating a unified governance model that improved visibility across its identity ecosystem while establishing a stronger foundation for future growth and evolving governance requirements. Standardized role-based access has also helped the organization strengthen governance while significantly reducing onboarding time for new employees.

Put your assessment to work

Organizations rarely maintain continuous compliance through periodic audit sprints. It begins with a unified identity security platform that provides ongoing visibility into who — or what — has access to critical systems, why that access exists, and whether it remains appropriate in real time.

Identifying your access gaps today is a critical step to help strengthen security, simplify audit preparation, and help reduce risk exposure as global regulatory expectations intensify.



[Discover how a modern identity security platform](#) can help your organization move away from fragmented, point-in-time audits and establish a stronger foundation to support your organization's compliance goals.

DISCLAIMER: THE INFORMATION CONTAINED IN THIS DOCUMENT IS FOR INFORMATIONAL PURPOSES ONLY, AND NOTHING CONVEYED IN THIS DOCUMENT IS INTENDED TO CONSTITUTE ANY FORM OF LEGAL ADVICE. SAILPOINT CANNOT GIVE SUCH ADVICE AND RECOMMENDS THAT YOU CONTACT LEGAL COUNSEL REGARDING APPLICABLE LEGAL ISSUES.