okta

Govern Every Identity: 5 Steps to Modernize your Identity Governance

In the modern landscape of rapid AI adoption and cloud sprawl, the traditional network perimeter has weakened, making identity governance the essential foundation of a secure environment. This checklist provides a strategic roadmap to audit your defense capabilities and bridge the gap between human and non-human security. By addressing these core categories, from initial inventory to automated lifecycle management, organizations can take steps designed to ensure that every identity — whether a human user, non-human identity (NHI), or AI agent — is accounted for, governed by least privilege, and continuously monitored for risk.

Inventory all identities

Establishing a single source of truth across your identity security fabric reduces blind spots created by shadow AI and unmanaged service accounts.

- ☐ Catalog every user, non-human identity (NHI), and AI agent
- ☐ Include both sanctioned and shadow accounts of any type
- ☐ Scan agent platforms (e.g., AWS Bedrock, Vertex AI, etc)
- ☐ Identify all identities (workforce and non-human) across cloud, on-prem, and SaaS platforms
- ☐ Detect orphaned or dormant accounts with no active owner
- ☐ Map each identity to the systems and data it can access

Assign human owners

Tying every digital entity to a responsible person validates that all automated actions remain grounded in a clear business context.

- ☐ Map every identity (human user, non-human identity (NHI), or AI agent) to a responsible person or team
- ☐ Document the business purpose for every identity
- ☐ Ensure ownership transfers when an employee changes roles or leaves
- ☐ Flag and suspend any identity without a valid, active owner

Okta Identity Governance

Enforce least privilege by automating user access reviews and provisioning.

okta

Apply least privilege

Moving toward a Zero-Standing Privilege (ZSP) model helps ensure that access is not persistent, which can significantly reduce the impact of compromised credentials.

- ☐ Grant access only for what is strictly needed, nothing more
- ☐ Use just-in-time (JIT) tokens instead of long-lived standing credentials
- ☐ Eliminate hardcoded API keys and static credentials in code or pipelines
- ☐ Ensure delegated and sub-agent access is narrower than the sponsoring identity's scope
- ☐ Enforce separation of duties (SoD) by identifying and remediating toxic access combinations

Standardize access reviews

Applying consistent certification standards across all identity types provides continuous validation that permissions remain aligned with actual business needs over time.

- ☐ Apply the same review and certification standards to service accounts and agents as to employees
- ☐ Run regular recertification campaigns for high-risk users and agents
- ☐ Actively check for SoD violations and conflicting entitlements across every identity in scope
- ☐ Revoke access that is no longer business-justified
- ☐ Flag any permissions that have expanded beyond their original scope
- ☐ Document and time-limit any exceptions, including approved SoD overrides

Automate lifecycle management

Automating the identity lifecycle, from Day 1 to offboarding, enables security to move at the speed of business without manual intervention.

- ☐ Route all identity provisioning through an approved request and workflow process
- ☐ Automatically deprovision credentials when a workflow, task, or employment ends
- ☐ Set credential expiration tied to role or task duration
- ☐ Trigger revocation of agent access when the sponsoring employee offboards
- ☐ Automate detection of unused or orphaned accounts across every identity type

Lifecycle Management

Automate the joiner, mover, and leaver process to eliminate manual effort and close security gaps.

okta

Maximize your governance strategy

Access our eBook on security-driven governance to help you modernize your governance posture. Learn how to transition from siloed, manual processes to automated resilience for every human user, non-human identity (NHI), and AI agent in your ecosystem.

Whether you have checked off most of these requirements or are just beginning to inventory your environment, Okta Identity Governance provides the strategic foundation needed to modernize your posture.

By transitioning from manual, siloed processes to a unified identity security fabric, your organization can automate the entire lifecycle for every human user, non-human identity, and AI agent.

Move beyond static permissions to a model of continuous, automated resilience that enforces least privilege and "Just-in-Time" access without slowing down your business.

Explore Okta Identity Governance

About Okta
Okta, Inc. is The World's Identity Company™. We secure AI, machine, and human identity so everyone is free to safely use any technology. Our customer and workforce solutions empower businesses and developers to protect their AI agents, users, employees, and partners while driving security, efficiencies, and innovation. Learn why the world's leading brands trust Okta for authentication, authorization, and more at okta.com.