Datasheet

November 2026

okta

Identity Governance: What you need to know

01 Why do growing companies struggle to track who has access to sensitive business data?

As workforces evolve, user roles shift while access permissions accumulate silently. This creates “access creep,” where employees retain unnecessary permissions long after role changes or departures. Okta® Lifecycle Management centralizes visibility into users’ access rights, showing not just who has access, but why and whether it’s still justified.

02 How can organizations prevent security breaches caused by active accounts of former employees?

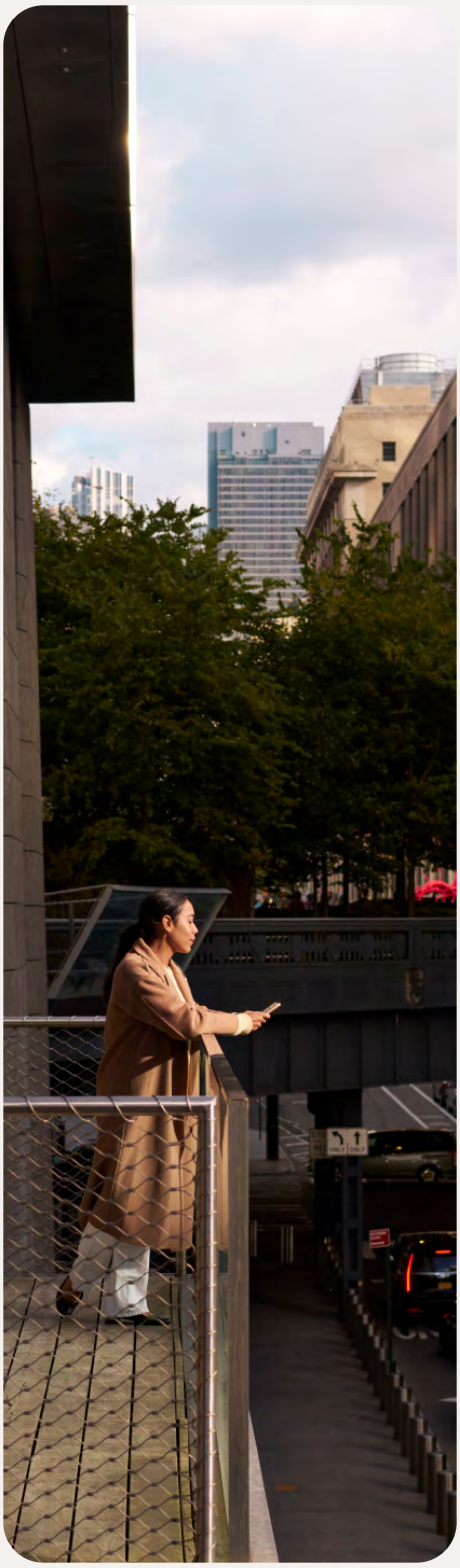
Manual offboarding processes routinely fail to comprehensively deprovision access, leaving orphaned accounts vulnerable to exploitation or insider threats. Okta Lifecycle Management automates the joiner, mover, leaver process, so when an employee leaves, application and system accounts they have are revoked instantly without manual intervention. Okta Workflows goes beyond standard joiner, mover, leaver processes into granular, multi-app orchestration, replacing fragile, manual scripts with robust automation to reduce operational friction. Additionally, Identity Security Posture Management can help discover and identify these orphaned accounts, so you don’t have to hunt them down.

03 What makes traditional compliance audits and access reviews so time-consuming and expensive?

Manual compliance reviews require teams to spend weeks tracking app owners, sending reminders, and combing through spreadsheets to reconstruct who has access to what and who approved what access. Okta Identity Governance automates access certification campaigns for identities across your enterprise, from humans to non-humans such as service accounts and AI agents. It then delivers review tasks directly to managers with usage context for more informed decision-making, cutting review cycles from months to days while producing audit-ready reports.

04 How do organizations prevent security silos when managing cloud applications alongside server infrastructure?

Managing identity with point solutions creates blind spots where privileged access goes unmonitored. Building a unified identity fabric can help prevent this, and Okta’s unified identity security platform can help organizations adopt this approach. For example, the Okta Platform brings together Okta Privileged Access and Okta Identity Governance, enabling you to apply access controls and least-privilege policies across identities (human, workloads, and AI agents) for consistent access management.



05 How can security teams mitigate the massive risks associated with administrative and highly privileged accounts?

Administrative and other privileged accounts are top targets because a single compromised credential can lead to a large-scale breach of the environment due to their privileged access. Security teams can reduce this risk in four steps: 1) Discover key privileged accounts, 2) Replace standing access with just-in-time and time-bound access where you can, 3) Vault and rotate the standing credentials you can't remove yet, and 4) Record and audit privileged sessions. Okta Privileged Access and Okta Identity Governance support these steps for humans, workloads, and AI agents, all of which use a single policy engine and audit trail.

06 How do you govern access when your workforce includes both human and non-human identities?

Traditional governance, designed only for human employees, overlooks non-human identities such as AI agents and service accounts, which are often provisioned and then forgotten without proper oversight. Okta Identity Governance extends the same least-privilege controls and lifecycle automation to all identity types, ensuring identities have a responsible owner and are continuously evaluated for access justification. Okta Privileged Access can extend those controls by providing a vault to store non-human identities and help ensure credentials are regularly rotated.

07 Why is a "single source of truth" for identities critical to governance?

When identity data is fragmented across HR systems, directories, and databases, governance teams lack visibility into who has access to what, making compliance audits highly complex and time-consuming, often requiring weeks of manual reconciliation. Okta Lifecycle Management and Okta Identity Governance pull user attributes and access from all identity sources (e.g., HR, Active Directory, cloud apps, on-premises systems) into a single control center, helping to ensure that access decisions are based on current, authoritative data.

08 How does governance contribute to reducing software spend and license waste?

Most organizations know who was provisioned software licenses but lack visibility into actual usage, leading to wasted spend on unused subscriptions and orphaned access that creates security risk. Okta Identity Governance can programmatically surface which licenses and access have gone stale or unused, enabling direct cost reduction without additional tools or new vendor relationships.

About Okta

Okta is The World's Identity Company™. We secure Identity, so everyone is free to safely use any technology. Our customer and workforce solutions empower businesses and developers to use the power of Identity to drive security, efficiencies, and success — all while protecting their users, employees, and partners. Learn why the world's leading brands trust Okta for authentication, authorization, and more at okta.com.