okta

AI Identity Security Compliance Checklist

Agentic AI is redefining identity security. While **91% of organizations** are deploying autonomous agents, nearly half lack formal oversight.[1] To bridge this gap, enterprises must integrate agents into existing identity frameworks, applying the same rigorous standards used for humans.

This checklist provides a unified strategy to move from shadow AI to a secure, enterprise-scale architecture by focusing on two pillars:

1. **Secure production-ready AI agents:** Move from AI pilot to secure production faster with agent interactions tied to human intent that are fully auditable.
2. **Govern all agents through a unified control plane:** Establish centralized visibility and control to secure the end-to-end lifecycle of agents across your environment.

For more on AI identity security, read the AI Agents in the Enterprise: The Security Risks Leaders Can't Afford to Miss whitepaper.

91% of organizations are deploying autonomous agents, but nearly half lack formal oversight.

[1] Okta, AI at Work 2025: Securing the AI-Powered Workforce

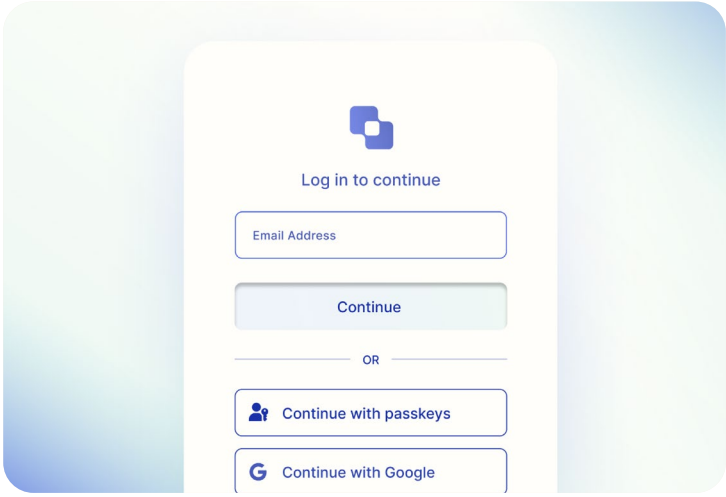
okta

The agentic AI governance checklist:

Secure production-ready AI agents

Authenticate

Authentication
Enforce sign-in via standard protocols (OIDC/OAuth 2.0) to help ensure every agent session is initiated by a verified human identity.
This prevents agents from acting under shared, generic identities and helps ensure accountability.



Authorize

Fine-grained authorization
Implement granular, relationship-based authorization for Retrieval-Augmented Generation (RAG) systems so agents only retrieve resources the specific user is permitted to see. By mapping agent scopes to the authenticated human's permissions, you help eliminate privilege escalation, even if an agent's logic is compromised.

Human-in-the-loop authorization
Require async approval for sensitive operations (e.g., deleting a database or spending >$1,000) using CIBA (Client-Initiated Backchannel Authentication) with Rich Authorization Request (RAR). This sends a real-time mobile authorization request for a specific action, creating a verifiable audit trail for security teams.

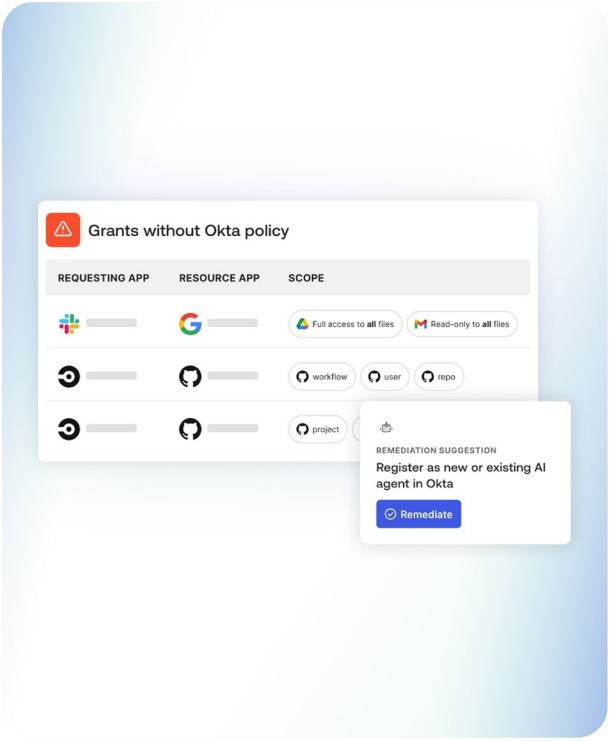
Token exchange
Share the user's identity in a more secure manner across different applications and trust domains. This maintains a verifiable link between the agent's actions and the human user, keeping the chain of user identity intact as the agent calls downstream APIs.

Secure

Token vaulting
Help eliminate credential leakage by securely storing OAuth tokens for third-party apps, APIs and MCP servers in a dedicated vault. Automatically refresh credentials so they do not appear in application code, logs, or LLM conversational outputs.

okta

Govern all agents through a unified control plane



Discover

Agent detection
Discover rogue agents across cloud and SaaS platforms. This reduces "Shadow AI" blind spots where unmanaged, over-privileged agents can otherwise act as invisible entry points for attackers.

Agent registry
Bring agents into your user directory and assign a unique identifier, owner, and documented purpose for each agent. Explicitly defining ownership and intent eliminates anonymity, making it possible to audit agent behavior.

Onboard

Privileged credentials
Secure agent credentials via a centralized vault and rotate them automatically (e.g., every 90 days). Treating secrets as ephemeral rather than static reduces the exploitation window for compromised credentials.

Access control
Implement granular, least-privilege permissions specifically tailored to each agent. Defining agent-specific access policies helps prevent lateral movement into sensitive systems outside its immediate scope.

Lifecycle management
Automate onboarding, access reviews, certifications, and deprovisioning to validate that permissions remain aligned with task requirements, helping maintain security across every stage of the agent's existence.

Protect

Universal logout
Implement immediate, cross-system revocation of sessions and access tokens when a threat is detected. Rapid containment helps prevent lateral movement across integrated SaaS and APIs while providing detailed logs for investigation.

okta

Bringing it all together: identity as the foundation of control

In the age of autonomous AI, identity serves as the central control plane that unifies visibility, control, and governance of human and non-human identities across your environment. By treating agents as first-class identities, organizations can bridge the governance gap and scale AI with confidence.

Secure production-ready AI agents

Category	Traditional Approach	Unified Identity Platform Capability
Authenticate	Agents act under a shared, generic identity (e.g., service account) with no direct link to a human user.	**Authentication:** Enforces sign-in via standard protocols (OIDC/OAuth 2.0) to help ensure every agent session is initiated by a verified human identity.
Authorize	Agents inherit broad, "all-or-nothing" read access to knowledge bases (over-privileged).	**Fine-grained authorization (FGA):** Tethers RAG retrieval to human permissions so that agents only access resources the specific user is explicitly allowed to see.
	Critical actions are either fully autonomous (risky) or blocked synchronously (slow/disruptive).	**Human-in-the-loop authorization:** Pushes real-time, out-of-band approval requests (via CIBA/RAR) to a user's mobile device for high-value or sensitive operations.
	The chain of user identity is broken as the agent calls downstream APIs and systems.	**Token exchange:** Shares the user's identity in a more secure manner across different applications and trust domains, maintaining a verifiable link between the agent's actions and the human user.
Secure	Tokens stored in configuration files or source code, creating risks of leakage in logs or LLM conversational outputs.	**Token vaulting:** Refresh tokens are offloaded to a more secure environment, issuing only short-lived access tokens so sensitive credentials remain outside the agent's execution context.

okta

Govern all agents through a unified control plane

Category	Traditional Approach	Unified Identity Platform Capability
Discover	Manual spreadsheets; blind spots regarding "Shadow AI" and rogue agents.	**Agent detection and registry:** Automatically discovers and registers agents (including metadata) in a central user directory for full visibility.
Onboard	Static credentials used indefinitely; rotation happens only after a breach.	**Privileged credentials:** Centralized policy enforces credential rotation (e.g., every 90 days) to limit exposure.
	Coarse-grained roles where agents inherit broad user permissions.	**Access control:** Enforces granular, least-privilege permissions tailored to the agent's scope to prevent lateral movement.
	Ineffective onboarding and manual reviews; obsolete agents retain access indefinitely.	**Lifecycle management:** Automated onboarding, access reviews, certifications, and deprovisioning to help ensure permissions are right-sized and stale agents are retired.
Secure	Manual investigation and fragmented revocation across different apps.	**Universal logout:** Immediate, cross-system revocation of sessions and tokens to contain threats instantly while providing detailed logs for further investigation.

AI Agents in the enterprise: the security risks leaders can't afford to miss.

Read the whitepaper

About Okta

Okta is the World's Identity Company. As the leading independent Identity partner, we free everyone to safely use any technology—anywhere, on any device or app. The most trusted brands trust Okta to enable secure access, authentication, and automation. With flexibility and neutrality at the core of our Okta Workforce Identity and Customer Identity Clouds, business leaders and developers can focus on innovation and accelerate digital transformation, thanks to customizable solutions and more than 7,000 pre-built integrations. We're building a world where Identity belongs to you. Learn more at okta.com.