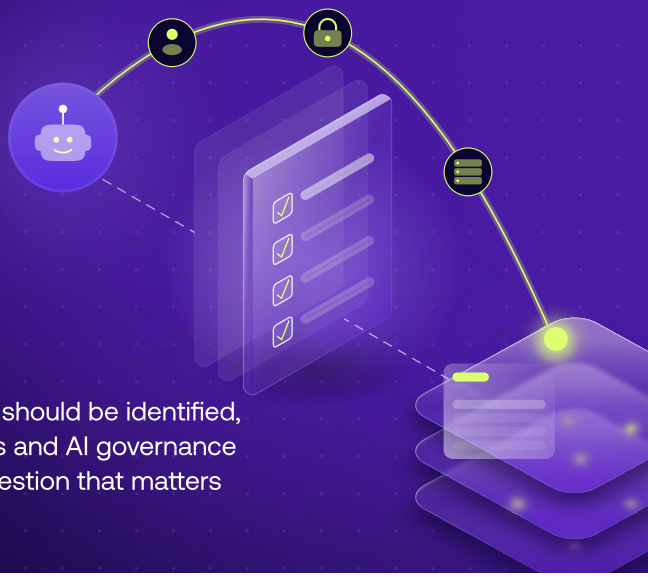
Orchid

Board Brief · Agent Identity

NIST's agent identity tenets: what the board should ask.



In October 2026, NIST proposed ten design tenets for how AI agents should be identified, authorized and audited. Expect them to appear in audit conversations and AI governance reviews. This page explains what they mean for oversight, and the question that matters more than compliance with them.

What NIST **proposed**

Agents should have their own verifiable identities, hold no standing privilege, receive short-lived access that can be revoked, operate under policy enforced outside the agent, and leave a record they can't alter.

These are initial design tenets published on NIST's blog, not a standard or regulation. They are a sound target for the agents your organization builds.

Why that's not the **whole picture**

The tenets describe the identity an organization gives its agent. Agents don't limit themselves to it. Given a goal, they use whatever access works, including old administrator accounts, logins that bypass single sign-on, and credentials nobody owns.

~5 min Average time for AI agents with a legitimate objective to find an alternate identity path and gain elevated access (Orchid research, 2026).

57% Share of enterprise identity that is unseen and unmanaged (Orchid Identity Gap 2026).

The question for the board

Not "do our agents meet NIST's tenets?" but "what access will our agents inherit, and who owns closing it?"

Three questions for **management**

1. **Coverage.** What share of the accounts inside our critical applications can we see and assign an owner to?
2. **Containment.** If an agent misuses access, how quickly can we revoke it, and where: only in our identity provider, or in the application itself?
3. **Evidence.** Can we show what an agent actually did, not only what it was permitted to do?

What good looks like in **90 days**

A baseline. An inventory of identity debt across the applications agents will touch first.

Owners. Each gap assigned to an existing function: identity, privileged access, governance or the SOC.

A score. Readiness measured against the tenets and reported on a regular schedule, like other risk metrics.

Source: NIST Cybersecurity Insights blog, "Design Tenets for Agent Identity Management Systems," Oct 27 2026. Summary is Orchid's paraphrase; NIST does not endorse Orchid Security. Self-assessment workbook: AI Readiness – Complete Enterprise Assessment Guide.