Sponsored content | White paper

The identity maturity curve: How to close gaps and gain value

CIO

Sponsored by opentext™

Identity at the center of security and business value

Identity and access management (IAM) has long been viewed as a gatekeeper — controlling who can access what systems, applications, and data. But in today's complex business environment, IAM is more than a security control. It is also a business enabler. The way organizations manage identity impacts productivity, compliance, user experience, and resilience.

Global research conducted by Foundry on behalf of OpenText shows that most enterprises are at a midpoint in their IAM journey. Many describe their maturity as "managed" or even "optimized." Yet the reality tells a different story: Identity remains one of the most common sources of security incidents, and the explosion of generative artificial intelligence (genAI) is raising both the stakes and the opportunities.

The organizations participating in the research reported that they had experienced an average of four identity-related incidents in the past 12 months. At the same time, 69% said that AI is accelerating adoption of adaptive, risk-based access controls. The message is clear: Identity is the frontline of enterprise security, and organizations must advance IAM maturity to keep pace with evolving risks.

The misconception: Maturity doesn't equal readiness

Many enterprises perceive themselves as mature in IAM. But the numbers reveal that foundational practices are still underused:

- **Just 36% of organizations enforce least-privilege access.**
- **Only 28% use just-in-time access models.**
- **A majority struggle with consistent policy enforcement across environments.**

This gap between perceived and actual maturity leaves organizations exposed. True maturity requires more than siloed controls. It requires integrated governance, automation, and adaptability across thousands of applications and identities — human and nonhuman alike.

Without this integration, organizations risk inconsistent audits, lingering access privileges, and "toxic combinations" of entitlements where a single individual can both create and approve transactions. These weaknesses undermine security and compliance, regardless of how mature the organization believes itself to be.

The challenges: Barriers slowing IAM progress

If the value of IAM is clear, why are so many organizations struggling to advance? The research points to three critical barriers:

- **Competing priorities:** 53% of the respondents cited conflicting IT and security agendas that stall progress.
- **Integration complexity:** 48% said connecting legacy and cloud systems into unified IAM programs is difficult.
- **Expertise gaps:** Among the less mature organizations, 47% reported lack of in-house expertise as a major barrier, compared to only 19% of the optimized organizations.

Mergers, acquisitions, and legacy infrastructure create silos of duplicate HR systems, identity stores, and manual processes. These factors make it challenging to enforce consistent controls at scale. The result is orphaned accounts, overprivileged users, and unmanaged third-party access — all of which increase risk.

Why focus now: Security, productivity, and resilience

IAM maturity delivers measurable value well beyond a reduction in incidents. In the research:

- **62% of the organizations reported improved productivity.**
- **61% cited stronger security outcomes.**
- **Large enterprises highlighted faster onboarding/offboarding and fewer compliance violations.**

IAM is not just about risk reduction but also about measurable business outcomes. Automated governance accelerates audits. Life cycle controls reduce human error. And passwordless authentication lowers help desk costs by reducing lockouts and resets.

In an era when AI is amplifying both opportunity and risk, the stakes are even higher. Among the responding organizations, 70% said AI is accelerating adoption of adaptive, risk-based controls. This means that identity programs must be ready not only to secure human users but also to govern an explosion of nonhuman identities: application programming interfaces (APIs), microservices, and AI agents acting on behalf of employees.

The ability to enforce real-time, context-aware access for humans as well as machines is quickly becoming the defining characteristic of mature IAM programs.

Communicating IAM value to business leaders

For IAM teams, proving value to boards and executives is as important as reducing incidents. The most effective communication ties identity initiatives directly to business outcomes:

- **Faster employee onboarding:** New hires are productive on day 1.
- **Audit readiness:** Processes that once took days now take hours.
- **Cost avoidance:** Reduced password reset volume lowers help desk expenses.
- **Strategic alignment:** IAM maturity supports merger-and-acquisition integration, zero-trust adoption, and digital transformation initiatives.

Executives respond to metrics that show operational impact: time saved, risks avoided, and compliance achieved. Positioning IAM in these terms reframes it from being a back-office function to becoming a strategic business enabler.

Closing the gaps, seizing the opportunity

IAM is no longer a "set it and forget it" function. It is a continuous journey that drives resilience, compliance, and competitiveness. Progress starts with closing maturity gaps through least-privilege and just-in-time access.

It also means tackling integration and expertise challenges with automation and trusted partners. And as AI expands the number of human and nonhuman identities, organizations must apply adaptive, risk-based controls to keep pace. Done well, IAM not only reduces risk but also builds trust, boosts productivity, and delivers lasting business value.

To reduce incidents and realize IAM's full potential, enterprises must make identity the center of their security and business strategy. **Learn how to** advance IAM maturity and build identity-centric resilience.