Buyers Guide

Enterprise IAM Evaluation Checklist

A practical IAM buyer’s guide for modern enterprises. Learn how identity, access governance, and lifecycle automation actually work at scale.

A practical framework for evaluating Identity and Access Management in modern enterprises

Identity and Access Management decisions tend to have long-term consequences. IAM platforms sit at the intersection of security, IT operations, compliance, and business productivity. This checklist is designed to help security and IT leaders evaluate IAM solutions based on real-world access risk, operational scalability, and architectural fit, not feature checklists alone.

Use this document to assess your current IAM posture or to compare vendors during an evaluation.

1. Identity Coverage & Scope

A strong IAM platform must govern access across all identities, not just full-time employees.

Evaluate whether the solution supports:

- Employees, contractors, and third-party users
- Privileged administrators and service operators
- Customers and external users (CIAM use cases)
- Non-human identities (service accounts, automation, APIs)

Key question:

Does the platform provide a unified access governance model across human and non-human identities, or does it require separate tools?

2. Integration with Your Existing Identity Stack

IAM rarely replaces existing systems. It must integrate cleanly with them.

Confirm support for:

- Active Directory and cloud directories
- Identity Providers (SSO, MFA, passwordless)
- HR systems as authoritative identity sources
- Cloud platforms and SaaS applications
- Disconnected or legacy systems

Key question:

Does the platform complement your IdP and HR systems, or attempt to replace them?

3. Identity Lifecycle Management (Joiner-Mover-Leaver)

Lifecycle automation is one of the most important predictors of IAM success.

Assess whether the platform can:

- Automatically provision access on day one
- Adjust access dynamically as roles change
- Immediately revoke access on termination
- Enforce least privilege throughout the lifecycle

Key question:

Is lifecycle enforcement continuous, or does it rely on periodic clean-up?

4. Self-Service Access & Approval Workflows

IAM should reduce friction without sacrificing control.

Evaluate capabilities for:

- User-driven access requests
- Policy-based approval workflows
- Time-bound and purpose-based access
- Full audit trails for all approvals

Key question:

Does self-service improve speed and governance, or simply shift risk to business users?

5. Access Visibility & Entitlement Intelligence

You cannot govern what you cannot see.

Confirm whether the platform provides:

- Clear visibility into who has access to what
- Insight into direct and indirect access paths
- Identification of excessive, dormant, or orphaned access
- Support for entitlement-level governance, not just roles

Key question:

Can security teams explain access decisions clearly to auditors and stakeholders?

6. Access Reviews & Certifications

Periodic access reviews are a compliance requirement—but also a risk signal.

Assess support for:

- Campaign-based and continuous access reviews
- Risk-prioritized review workflows
- Delegation to application owners and managers
- Evidence capture and audit reporting

Key question:

Are reviews a once-a-year checkbox, or an ongoing governance mechanism?

7. Privileged Access Management (PAM)

Privileged access represents the highest-risk identities.

Evaluate whether the solution supports:

- Just-in-time privileged access
- Approval-based elevation
- Time-bound permissions
- Elimination of standing admin access

Key question:

Does the platform reduce privilege by design, or simply store credentials more securely?

8. Support for Disconnected & Legacy Systems

High-risk access often lives outside modern SaaS platforms.

Confirm support for:

- CSV-based or API-light integrations
- Browser-based or headless automation
- On-premise and custom-built applications
- Manual systems brought under governance

Key question:

Does the IAM program stop at “what’s easy,” or cover what matters most?

9. Deployment & Architecture Flexibility

IAM is foundational infrastructure. Deployment options matter.

Evaluate availability of:

- SaaS deployment
- Customer-managed cloud deployment
- On-premise installation
- Air-gapped environments

Key question:

Is the same software and capability available across deployment models?

10. Compliance, Audit & Reporting

IAM should make audits easier not harder.

Assess whether the platform provides:

- Built-in compliance reporting
- Evidence collection for access decisions
- Support for common audit frameworks
- Real-time visibility into access posture

Key question:

Can auditors self-serve answers, or does every audit trigger manual work?

11. Scalability & Operational Overhead

IAM must scale with the organization.

Evaluate:

- Time to onboard new applications
- Effort required to maintain integrations
- Dependency on professional services
- Impact on IT and security team workload

Key question:

Does the platform reduce operational burden as you scale or increase it?

12. Buyer Red Flags to Watch For

During evaluation, watch for these common warning signs:

- IAM positioned purely as SSO or MFA
- Heavy reliance on static groups
- Privileged access solved only through password vaulting
- Limited support for legacy or disconnected systems
- Governance features gated behind costly add-ons

Final Self-Assessment

Before selecting an IAM platform, ask:

- Can we explain why every identity has access?
- Can we revoke access instantly, everywhere?
- Can we prove access decisions to auditors without scrambling?
- Does this architecture still work at 2× or 5× our current scale?

If the answer to any of these is “not confidently,” IAM maturity (not tooling) may be the real gap.

Next step:

Use this checklist to score vendors and identify gaps in your current IAM program. The goal is not feature parity, it is sustained access governance at enterprise scale.

Interested in learning more?
Schedule a demo.

Let us know where to reach you and a member of our team will contact you soon to schedule a time to walk through our solution!

Request a Demo