Everyday Identity

Breaking down identity, one post at a time.

IAM Health Check Checklist

Overprovisioned Access

□ Are access reviews conducted quarterly?

□ Are admin roles scoped appropriately to least privilege?

Inconsistent MFA Enforcement

□ Are all users (internal and external) protected by enforced MFA?

□ Are phishing-resistant MFA methods (like FIDO2) used instead of SMS where possible?

Orphaned Accounts

□ Are orphaned or inactive accounts disabled immediately after offboarding?

□ Is there an automated integration between HR systems and IAM for user lifecycle management?

Poorly Configured Delegated Admin Access

□ Is admin activity regularly audited and reviewed?

□ Are delegated admin roles granular and appropriately scoped (e.g., no unnecessary global admin rights)?

Lack of Session Management

□ Is session timeout configured for sensitive applications?

□ Is step-up authentication enforced for high-risk or sensitive transactions?

Inadequate Logging and Monitoring

□ Are IAM logs centralized and monitored daily?

□ Are alerts set for identity-based anomalies (e.g., impossible travel, privilege escalation)?

Weak Identity Federation Trust

□ Are federated external IdPs audited at least twice a year?

□ Are strong federation trust policies enforced (e.g., MFA requirement, encrypted assertions)?

Quick Tip:

Aim for 90%+ compliance across all categories to dramatically lower your identity-related security risk.