Frontier Identity

IAM · M&A · DUE DILIGENCE

The IAM M&A Due Diligence Checklist

A practitioner's checklist for assessing a target company's identity & access posture before close.

Most diligence underwrites financials, contracts, and the tech stack. Identity and access management rarely gets the same scrutiny, yet it carries breach exposure, audit findings, and integration cost that all land on the acquirer after close. Use this checklist during the diligence window to turn unknown identity risk into a priced, planned line item. It follows the order a real assessment runs in: discover the estate first, then work the highest-risk areas, then read the signals that drive integration cost.

1 · Identity Estate & Directory Discovery

You cannot assess what you have not mapped. Establish the full footprint first.

- [ ] Inventory every directory and identity provider (Active Directory, Entra ID, Okta, Ping, LDAP, Google).
- [ ] Identify the authoritative sources of identity (HRIS feeds, contractor systems) and how they sync.
- [ ] Find shadow and legacy directories and standalone app-level identity stores not on any diagram.
- [ ] Separate human identities from non-human ones (service accounts, machine, API, and workload identities).
- [ ] Document domain/forest trusts, federation relationships, and any cross-org access that already exists.
- [ ] Catalog external, guest, vendor, and B2B identities that hold access to internal systems.

2 · Privileged Access & Entitlements

Privilege is where breach impact concentrates. This is the highest-value section.

- [ ] Enumerate privileged and administrative accounts across domains, cloud, SaaS, and infrastructure.
- [ ] Distinguish standing (always-on) privilege from just-in-time / time-bound access.
- [ ] Confirm whether a PAM solution exists and what share of privileged accounts it actually vaults.
- [ ] Locate shared, generic, and break-glass admin accounts and how their credentials are controlled.
- [ ] Look for over-provisioned access and entitlement creep (access that no longer matches the role).
- [ ] Assess segregation-of-duties conflicts in high-risk areas (finance, production, identity itself).

3 · Authentication & External Exposure

The most common path to compromise, and the easiest to evidence in diligence.

- [ ] Measure MFA coverage separately for workforce, administrators, and remote/VPN access.

- [ ] Identify legacy or weak authentication still in use (NTLM, basic auth, legacy mail protocols).
- [ ] Review password policy, credential hygiene, and exposure in known breach corpuses.
- [ ] Map externally exposed authentication surfaces (VPN, RDP, webmail, admin portals).
- [ ] Quantify SSO coverage and count business-critical apps that sit outside SSO.
- [ ] Assess conditional access / zero-trust posture (device, location, and risk-based controls).

4 · Identity Lifecycle & Governance

Weak lifecycle controls are the root cause of most orphaned-access risk.

- [ ] Evaluate joiner-mover-leaver (JML) maturity: how much is automated versus manual or ticket-driven.
- [ ] Quantify orphaned and dormant accounts, especially for departed employees and contractors.
- [ ] Review access request and approval workflows and whether approvals are meaningful or rubber-stamped.
- [ ] Confirm access certification / recertification campaigns run, and how exceptions are handled.
- [ ] Assess the role and entitlement model (RBAC): whether one exists, how accurate it is, and how far it has sprawled.
- [ ] Check deprovisioning timeliness against a defined SLA (hours, not weeks, for high-risk roles).

5 · Compliance & Audit Posture

Findings here often resurface immediately post-close, when scrutiny is highest.

- [ ] Identify applicable regimes (SOX, HIPAA, PCI DSS, GDPR, sector-specific) and IAM-relevant controls.
- [ ] Review recent audit findings and unresolved remediation items related to access control.
- [ ] Confirm access reviews, logging, and monitoring produce evidence an auditor would accept.
- [ ] Request the history of identity-related incidents, breaches, and near-misses.
- [ ] Check cyber-insurance requirements tied to IAM controls (MFA, PAM) and any coverage gaps.

6 · Integration Cost & Complexity Signals

Put findings in terms the deal model can use: cost, effort, and risk.

- [ ] Gauge directory consolidation complexity (overlap, naming conflicts, duplicate identities).
- [ ] Identify tooling overlap and redundant IAM / PAM / SSO licensing across both entities.
- [ ] Flag end-of-life or unsupported identity systems that force near-term replacement.
- [ ] Estimate remediation effort for the critical gaps surfaced above (rough order of magnitude).
- [ ] Test the feasibility of a secure Day-1 access model given the current state.
- [ ] Assess key-person and operational dependency risk within the target's identity team.

Turning the checklist into a number

A checklist surfaces issues; diligence prices them. Each gap above maps to a cost (remediation, tooling, effort) and a risk (breach exposure, audit finding, integration delay) that belongs in the deal model rather than in a surprise after close. Frontier Identity runs this assessment as a focused engagement and delivers a risk-ranked findings report and an integration cost estimate the deal team can act on before the number is locked.

Book a discovery call → frontieridentity.com