rubrik

Identity Security Checklist: 9 Steps to Identity Resilience

“Identity is the new perimeter”—today, that goes without saying. But how do you truly fortify this new perimeter across sprawling, hybrid identity environments?

This guide outlines 9 critical areas every organization should explore to secure human and non-human identities, strengthen hybrid IAM, and build resilience for fast recovery after a breach.

Read on to start building true Identity Resilience against today’s most sophisticated attacks.

1 CENTRALIZE IDENTITY VISIBILITY ACROSS HYBRID IDPS

The Risk:

Many organizations manage fragmented identity landscapes involving multiple Identity Providers (IDPs) such as Active Directory (AD), Entra ID, Okta, and AWS Identity Center. Older, legacy identity systems often remain intertwined with newer ones, creating difficult dependencies. Adding new technologies further escalates the complexity of managing identities, permissions, and access consistently.

What to Do:

- **Establish a unified view:** Implement a solution providing centralized identity visibility across all your Identity Providers (IDPs) to avoid missing critical gaps and inconsistent policies.
- **Choose flexible integration:** Select tools that integrate across multiple IDPs (such as Okta, Entra ID, and Active Directory) without locking you into a single vendor, streamlining governance and reducing configuration sprawl.

Why It Matters:

Centralized visibility enables faster remediation of identity-related gaps or inconsistent policies, reducing hidden vulnerabilities that can compound over time across your identity environment.

2 BREAK DOWN IAM SILOS: ALIGN IT AND SECURITY

The Risk:

Traditionally, Identity and Access Management (IAM) was solely an IT function, focused on provisioning and usability. However, the surge in identity-related attacks has made IAM critical to overall security. IT-centric IAM initiatives often lack the security context needed to address modern threats, such as insights into vulnerabilities, attack paths, and recent threats.

What to Do:

- **Bridge IT and Security:** make IAM a shared responsibility.
- Ensure the CISO and security teams shape IAM policy, operations, and tooling decisions.

Why It Matters:

Close collaboration helps IT and security teams effectively manage and secure identities and keep pace with the broader organization adopting new technologies.

3 PRIORITIZE SECURITY FOR CRITICAL APPS WITH SENSITIVE DATA

The Risk:

Not all apps are equal—losing access to platforms like Salesforce, Workday, or AWS hits harder than some internal tools. These critical applications often rely on unmanaged, app-defined identities (e.g., service accounts, API keys).

What to Do:

- Label app criticality and assess for sensitive data (PII, IP, financials).
- Map and assess all connected identities—including app-native ones.
- Evaluate identity configuration and data access exposure.

Why It Matters:

Context-aware identity controls reduce blast radius and ensure your most vital systems remain protected.

4 EXPAND FOCUS BEYOND ADMINS TO OTHER CRITICAL IDENTITIES

The Risk:

While security teams naturally focus on admins, significant risks also exist in other areas. For example, an IT user might have excessive permissions to modify Active Directory, or a data scientist could be overly exposed to sensitive data. If compromised, these overlooked identities can lead to leaving backdoors, creating persistence creating further damage than initially perceived.

What to Do:

- Clearly identify all sensitive identities according to their impact within your environment:
  - Map identities clearly to their actual privileges, understanding precisely what their permissions permit them to do.
  - Connect identities directly to your sensitive data, assessing how easily critical information could be accessed, misused, or deleted if compromised.

Why It Matters:

Prioritizing sensitive identities reduces overlooked attack paths, clarifies potential blast radius, and enables faster containment during incidents.

5 DISCOVER, MONITOR, AND SECURE NON-HUMAN IDENTITIES (NHIS)

The Risk:

Non-Human Identities (NHIs), such as service accounts, bots, API tokens, and AI agents - are exploding, often outnumbering human identities 50:1, creating a massive, frequently unmanaged attack surface. Their high privileges and ephemeral nature make NHIs prone to leakage through code, logs, and CI/CD pipelines, where a single compromised credential can grant attackers broad access and enable rapid escalation.

What to Do:

- **Discover & Enforce Least Privilege:** Continuously inventory all NHIs and enforce least privilege, granting only essential permissions.
- **Automate Lifecycle & Credential Management:** Automate provisioning, de-provisioning, and rotation of NHI credentials, centralizing them securely.
- **Monitor & Segment:** Continuously monitor NHI behavior for anomalies and use network segmentation to limit blast radius.

Why It Matters:

NHI risks are fundamentally identity risks and must be managed through a holistic identity security approach, especially as environments become increasingly automated and potentially populated with AI agents.

6 ELIMINATE STALE AND DORMANT ACCOUNTS

The Risk:

Orphaned and stale accounts are prime attacker targets. They often have old passwords, unused permissions. Attackers exploit them to gain initial access and move laterally.

What to Do:

- **Establish clear inactivity policies:** for example, disable accounts after 90 days of inactivity, then delete them after 180 days. Regularly review user permissions with time, as users rarely end up with less access when changing roles or teams.
- **Integrate lifecycle management:** Implement automated processes to securely bridge Human Resources (HR) systems and Identity Providers (IDPs). Security teams often build lightweight internal automations - for example, leveraging no-code platforms like n8n to streamline account deprovisioning.

Why It Matters:

Consistently managing inactive accounts reduces easy entry points, limiting attackers' opportunities for initial access and internal movement.

7 MOVE BEYOND AUDITS TO ACTIONABLE INSIGHTS AND REMEDIATION

The Risk:

While audits excel at identifying issues (e.g., users lacking MFA), they often fall short on providing actionable remediation steps. Additionally, certain service accounts or business groups can't always utilize MFA.

What to Do:

- **Prioritize audit findings starting with high-impact identities.** If an audit identifies indicators of exposure (IOEs) for specific users, prioritize remediation by starting with the most sensitive identities (as noted in point 4, sensitive identities aren't limited to admins and executives).
- **Address MFA exceptions proactively:** Where MFA implementation isn't feasible, establish robust monitoring of these identities and configure specific Security Information and Event Management (SIEM) rules to promptly detect and respond if compromised.

Why It Matters:

Action-oriented remediation ensures findings lead to real risk reduction, not just checkbox compliance.

8 MONITOR, REMEDIATE, AND RAPIDLY REVERT CRITICAL IDENTITY PROVIDER CHANGES

The Risk:

Unnoticed or mismanaged changes to your identity providers (e.g., Active Directory (AD) Group Policy Object (GPO) edits or Entra policies) can create severe security gaps. Unexpected changes can also signal attacker persistence or lateral movement.

What to Do:

- **Implement proactive alerting:** Use solutions that immediately alert your team when critical identity configuration changes or unusual activity occurs, such as GPO changes outside maintenance windows or new policies granting admin access.
- **Rapidly remediate:** Ensure the solution that provides straightforward, one-click remediation to revert unwanted or unauthorized changes, restoring "clean-state" configurations quickly.

Why It Matters:

Quick detection and the ability to rapidly remediate by reverting harmful changes significantly limit your exposure to attacker activities or damaging misconfigurations.

9 PLAN FOR BREACH: ASSUME COMPROMISE AND ENABLE IDENTITY RECOVERY

The Risk:

A breach is inevitable - it's a matter of when, not if. When a full-scale attack targets your Active Directory forest, your recovery speed dictates the extent of damage. During an attack, relying on complex multi-vendor processes or non-resilient backups will extend recovery time; hoping for the best isn't an identity recovery plan.

What to Do:

- Choose identity recovery solutions specifically designed to withstand attacks themselves, ensuring they remain secure, operational, and available—even when your environment is compromised.
- **Ensure Multi-IDP Support and Reliable Synchronization:** Choose solutions that can reliably synchronize identities and configurations post-recovery for multiple IDPs (e.g. syncing AD and EntraID)
- **Pinpoint compromise and enable easy remediation:** In case identities are compromised, make sure your recovery solution clearly identifies exactly which identity attributes changed and enables rapid, straightforward remediation.

Why It Matters:

Rapid, effective recovery capabilities directly reduce downtime and impact to the business.

BUILD IDENTITY RESILIENCE WITH RUBRIK

Rubrik delivers modern identity resilience—bringing together:

- Orchestrated identity recovery across AD, Entra ID, and hybrid environments
- Posture and hygiene monitoring for both human and non-human identities
- Risk-driven remediation that prevents compromise before it spreads
- Actionable insights into identity exposure, misuse, and blast radius

With Rubrik, you can secure identity infrastructure *before*, *during*, and *after* an attack.

Reach out to us today to learn how Rubrik can help you build cyber resilience.

rubrik

Global HQ
3495 Deer Creek Road
Palo Alto, CA 94304
United States

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com

ds-identity-security-checklist / 20250609