Omada

Identity Risk Scorecard — Board Handout

Purpose

A concise, executive-level view of identity exposure and governance, designed to surface risk and remediation trends for board and executive discussions.

Identity Risk Scorecard (monthly)

Risk Exposure
What access risk exists today?

- **Privileged accounts inactive > 90 days** % of high-impact accounts that remain active despite no recent use.
- **Orphaned / ownerless accounts (count & trend)** Accounts with no clearly assigned business or technical owner.

Exposure Window
How long does access-related risk persist?

- **Mean time to revoke access (MTTR)** Average time to remove access after termination or role change (employees, contractors, non-human identities).

Scale & Control
How large and governable is the attack surface?

- **Non-human–to–human identity ratio (measured)** Service accounts, APIs, bots, and AI agents compared to employees and contractors.
- **Credential rotation coverage (non-human identities)** % of non-human identities using rotating or short-lived credentials.

Governance Signal
How effectively is identity risk being resolved?

- **Open identity-related audit findings (count & aging)** Number and age of unresolved identity findings, showing remediation discipline over time.

How boards should use this scorecard

- Review trends over time, not single data points.
- Expect a named owner, a target/threshold, and a one-line interpretation for each metric.
- Use this view to inform investment, prioritization, and risk acceptance decisions at the executive level.

Quick interpretation examples

- Rising privileged inactivity increases potential blast radius if credentials are abused.
- Long MTTRs indicate extended exposure to insider and third-party risk.
- Rapid growth in non-human identities without credential rotation or clear ownership increases the unmanaged attack surface.

This scorecard reflects widely accepted executive guidance on outcome-based identity reporting and is informed by practical experience working with security and identity leaders in complex, regulated environments.