Tracking What **Matters**

Board-Level Identity Metrics for Modern Identity Security

Identity security programs often struggle not because teams lack effort or tools, but because the value of identity risk reduction is difficult to communicate at the executive level. This guidance is intended to help security and identity leaders elevate those conversations, regardless of technology choices, by focusing on the metrics that matter most to boards.

Why Identity Metrics Fail the Board

Boards are not under-investing in identity security because they don't care. They are under-investing because they are shown identity **activity metrics**, not risk **exposure metrics**.

For years, identity reporting has focused on what is easy to count:

- Provisioning and deprovisioning SLAs
- Certification completion rates
- Ticket volumes and tool adoption

These measures describe **process efficiency,** not **risk posture**.

The Omada State of IGA 2026 report shows why this gap matters now more than ever:

- **Identity environments have scaled beyond human-centric governance.** Non-human identities, including service accounts, APIs, bots, and AI agents, now outnumber human identities by orders of magnitude, expanding the identity attack surface far beyond traditional oversight models.
- **Agentic AI increases autonomy faster than governance can adapt.** Security leaders cite misuse of agent autonomy and loss of human oversight as top concerns, reflecting growing risk as autonomous identities act independently across critical systems.
- **Executive visibility has not kept pace with either scale or autonomy.** More than 40% of executives cannot answer basic questions about privileged access exposure, orphaned accounts, or how long access persists after people leave. Boards invest to manage risk. If reporting emphasizes activity, identity is treated as an efficiency issue. If reporting emphasizes exposure, identity is treated as a security issue.

This guide is designed as a practical tool for CISOs and IAM leaders to shift board conversations from *"Are we efficient?"* to *"Are we exposed?"*

The Metrics That Change Board Decisions

Stop Reporting Activity. Start Reporting Exposure.

Activity metrics are necessary, but insufficient for understanding identity risk.

Not all identity metrics are equal. A small number consistently predict breach likelihood, audit friction, and incident impact.

Stop Emphasizing ⟶ Start Tracking

Commonly Emphasized	What It Misses	What to Track Instead	Why Boards Care
Provisioning SLAs	Excess access accumulation	**Privileged access coverage** (how many accounts are unused >90 days but still active)	Reveals latent blast radius if credentials are abused
Certification completion	Whether access was reduced	**Orphaned / ownerless account trends**	Signals unmanaged attack paths
Deprovisioning SLA	Duration of risk	**Mean time to revoke access (MTTR)**	Measures exposure window after termination
Ticket volumes	Risk concentration	**High-risk identity count**	Shows where controls are weakest
IGA tool rollout	Whether controls are reducing risk	**Credential rotation coverage (NHIs)**	Shows whether deployed tools are actually eliminating static, long-lived access risk

Discipline matters. Boards do not need dozens of KPIs. They need a short list of metrics that clearly answer:

- **How much identity risk exists today?**
- **Is it increasing or decreasing?**
- **Who is accountable for improving it?**

The Board-Ready Identity Risk Scorecard

In addition to exposure metrics that replace activity reporting, boards should also see a small number of governance health indicators, including open identity-related audit findings, which show whether identified identity risks are being remediated over time rather than simply assessed at a point in time.

Identity Risk Scorecard (Monthly)

This scorecard is designed to support board and executive discussions, not to replace operational dashboards.

Risk Exposure

- % of privileged accounts inactive >90 days
- Orphaned / ownerless accounts (count and trend)

Exposure Window (how long access-related risk persists)

- Mean time to revoke access (employees, contractors, non-human identities)

Scale & Control

- Non-human identity to human identity ratio (service accounts, APIs, bots, and AI agents compared to employees and contractors, measured not estimated)
- % of non-human identities using rotating credentials

Governance Signal

- Open identity-related audit findings (count and aging)

Each metric should include:

- An assigned owner
- A sensible target or threshold
- A six-month trend line
- A one-line interpretation in business language

Example:

"Our average access revocation time is 36 hours, meaning terminated users retain access for a day and a half. Our target is under 8 hours."

This format allows boards to assess identity risk **without becoming identity experts.**

Using Metrics to Influence Investment

Turning Visibility into Action

Identity metrics are most powerful when explicitly tied to investment outcomes.

The value of identity metrics comes from consistent measurement paired with audience-appropriate interpretation.

For CISOs

Use exposure metrics to justify:

- Automation investment to shrink access exposure windows and limit blast radius when identities are misused
- Platform consolidation to right-size entitlements and eliminate ownerless access paths
- Funding for non-human identity governance to maintain human oversight as AI agents and automation expand

Reframe the conversation:

- Not "We need better IGA tooling"
- But "We are carrying unnecessary access exposure that increases breach and audit risk."

For IAM / IGA Leaders

Use the same metrics to show value upward:

- Demonstrate how identity controls reduce exposure windows
- Show declining orphaned accounts and privileged access risk over time
- Position IGA as an enabler of security and AI-driven automation

Translate technical results into business outcomes:

- "We reduced the window attackers could exploit access by 70%."
- "We eliminated 40% of ownerless machine identities tied to audit findings."

Getting Started

The First 90 Days

Progress does not equal instant perfection. The objective is momentum and visibility.

Step 1: Add Two Metrics

Introduce just two exposure metrics into existing executive reporting:

- Privileged access coverage
- Mean time to revoke access

Step 2: Assign Accountability

Each metric must have:

- An operational owner
- An executive sponsor

Step 3: Baseline and Trend

Initial numbers will be uncomfortable. That is the point. Trend lines matter more than starting values.

Identity security governance becomes strategic when leaders have clear visibility into risk, discuss it consistently, and invest deliberately, rather than reacting after incidents or audits force the issue.

Final Thought

Boards invest in what they can see. When identity metrics reveal exposure instead of activity, identity security earns its place alongside financial, operational, and strategic risks on the executive agenda.

Organizations that consistently use these metrics find that identity security becomes easier to fund, easier to govern, and easier to scale, because its impact is visible in the language executives already use to manage risk.

This guidance is informed by Omada's work with identity and security leaders across highly regulated enterprises.

Start with the Board-Ready Identity Risk Scorecard

Use this one-page scorecard to introduce exposure-focused identity metrics into executive reporting and begin building trend-based visibility.