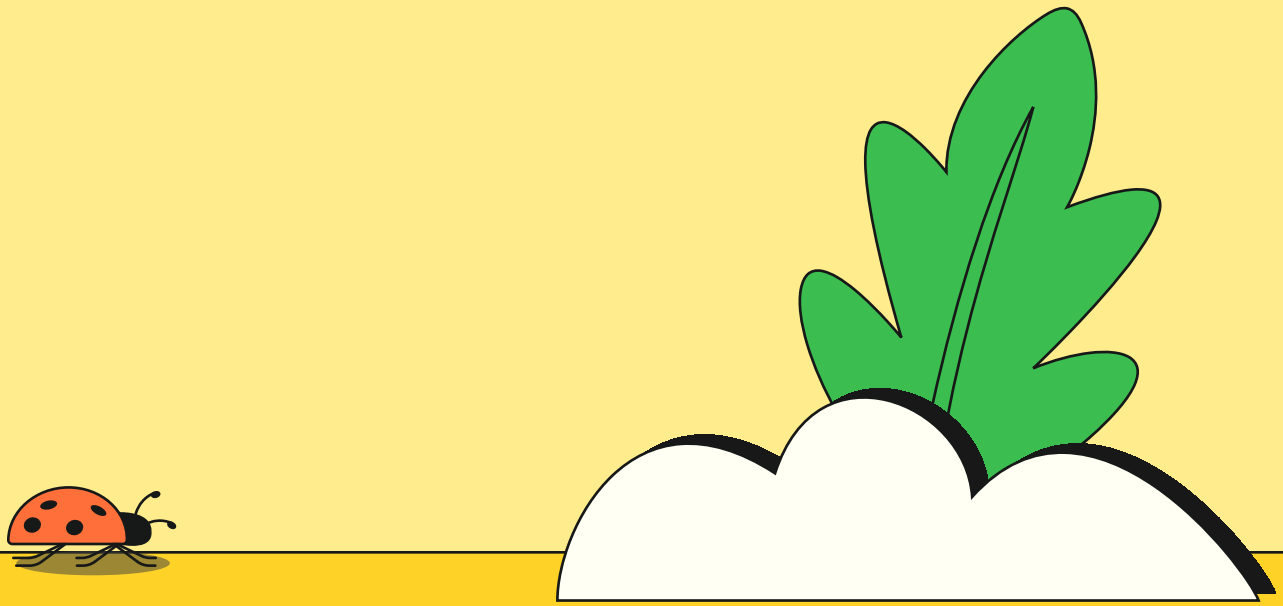
GUIDE

The CISO's Guide to Modern Identity Governance

Why identity governance maturity has become table stakes for security and operational continuity

LINX

Table of Contents



Executive Summary

The challenge facing CISOs is no longer identity management. It is identity governance. Most organizations have invested heavily in identity controls, from multifactor authentication (MFA) to single sign-on and beyond, yet far fewer can confidently answer who has access to what, why they have it, whether that access remains appropriate, and what risk it creates across a sprawling digital estate.

The average enterprise now operates nearly 900 applications, but according to Salesforce's Mulesoft Connectivity Benchmark Report, only 29% are connected to the central integration platforms security teams rely on as the source of truth for assessing governance coverage. This explains why a UnitedHealth server with direct access to sensitive, critical data stores was running without MFA. You cannot govern what you cannot see, and that visibility blind spot is the root of the problem CISOs now face.

This paper examines how fragmented identity ecosystems, entitlement sprawl, manual lifecycle processes, growing third-party access, least-privilege implementation obstacles, and non-human identity risk are widening the gap between *perceived* access and *actual* access. It argues that modern security leaders can no longer view identity governance as a compliance function. CISOs today must fully embrace it as a measure of enterprise resilience, operational stability, and risk management effectiveness.

Questions this guide will answer

Why are traditional controls like MFA, SSO, and PAM failing to prevent enterprise identity breaches, and why are major incidents at Change Healthcare, Snowflake, and MGM Resorts fundamentally identity governance failures?

How do fragmented identity data, entitlement sprawl, manual certification campaigns, and non-human identities (outnumbering human identities 144:1) create operational blind spots across modern enterprise environments?

What specific operational, security, and resilience benefits do enterprises gain when transitioning from static compliance reviews to continuous, AI-driven identity governance?

How can security leaders evaluate their current posture across the four levels of the Governance Maturity Map to build an adaptive, risk-informed identity governance and administration (IGA) program?

Identity Is the Control Plane Attackers Target First

Modern enterprise perimeters have dissolved into millions of real-time access decisions across hybrid, multi-cloud, and SaaS environments. Identity is no longer just a component of your infrastructure. It is the primary control plane, and consequently, your largest and most active attack surface.

Threat actors no longer need to break through a firewall when they can simply log in using valid, ungoverned credentials; authentication without continuous governance is merely a false sense of security.

For example, the Change Healthcare attack affected hospitals, insurers, pharmacies, and over 100 million individuals. A **single set of compromised credentials** took hundreds of U.S. healthcare institutions offline, halting all patient intakes, diagnostics, surgeries, and claims processing. One of the most consequential cyberattacks on record, it started with *one identity* nobody was watching closely enough.

Three months later, attackers used credentials harvested by **infostealer malware to access customer environments hosted on Snowflake.** As with Change Healthcare, identities that appeared legitimate moved through trusted systems unchallenged, exposing data from more than 165 organizations before most victims knew they had a problem.

The MGM Resorts breach took a different path. No stolen credentials, no compromised identities, no missing **MFA**. Attackers instead convinced MGM's help desk to reset valid credentials, exploiting a trusted operational process rather than a technical gap. That single foothold triggered large-scale operational disruption across one of the world's biggest hospitality brands.

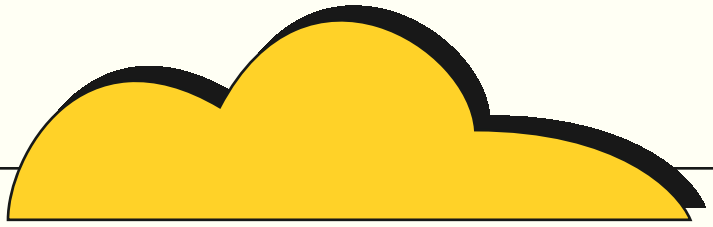
The One Common Culprit: Governance Visibility

While the victims across the above three attacks were different, the vector was identical: **identity**. None of these organizations lacked identity controls. All three, and most other enterprises, have invested heavily in **MFA**, **SSO**, **PAM**, and **Zero Trust** initiatives. The failure point arises when governance visibility breaks down between authentication, authorization, and ownership, with attackers exploiting that exact seam.

Microsoft's 2024 Digital Defense Report quantifies the scale: over 600 million identity-related attacks detected every day, and more than 7,000 password attacks blocked every second. **Verizon's 2025 data** confirms the trend is accelerating, with **60%** of breaches involving the human element and credential abuse remaining one of the most common intrusion paths at **32%**.

Malicious actors exploit identity governance whenever adversaries acquire and use legitimate credentials. **For today's CISO, identity governance must evolve beyond a compliance feature into a strategic security function.** One that can answer for every login and every identity, and know whether access should exist and what it permits. Every single time.

The sections that follow unpack where enterprise visibility breaks down in practice, and how forward-looking security leaders can bridge the gap between authentication and continuous authorization.



The Top Six Identity Governance Challenges CISO's Currently Face

According to 2025 data from Salesforce, the average enterprise operates **nearly 900 apps.** Yet fewer than a third (**29%**) connect to the platforms that security teams rely on to implement and assess governance coverage. This is why the six challenges below keep recurring across every breach disclosure, regardless of industry.

1 When Identity Data Is Fragmented, Governance Becomes Guesswork

Years of cloud adoption, acquisitions, SaaS expansion, and technology modernization have left organizations managing identities across multiple directories, identity providers, and platform-specific access models. According to a **2025 Cloud Security Alliance (CSA) survey**, **75%** of organizations now rely on two or more identity providers, while **11%** operate five or more.

Most enterprises did not intentionally create these fragmented identity ecosystems. They evolved into them. The bottleneck is that governance can only be as complete as the identity data it can see.

Although standards such as **SAML**, **OIDC**, and **SCIM** were designed to improve interoperability, inconsistent implementation across vendors continues to create integration gaps. CSA's 2025 survey also noted that nearly **6 in 10 enterprises** report moderate to high difficulty onboarding on-premises applications into cloud identity providers.

As a result, identity data becomes fragmented across cloud, hybrid, SaaS, third-party, and AI environments.

The Change Healthcare breach illustrates the cost of these governance blind spots. Unbeknownst to UnitedHealth, one of America's largest healthcare payment networks, a server connected to critical data stores lacked **MFA**, allowing attackers to simply log in with stolen credentials. The resulting compromise caused widespread operational disruption, regulatory scrutiny, and reputational damage, demonstrating how identity failures can threaten business continuity and patient safety.

One of the foundational principles Linx emphasizes when it comes to **identity governance** focuses on this issue: Before organizations can govern access consistently, they must first establish a reliable understanding of **where identities, permissions, and trust relationships actually reside.**

Questions to ask:

Could you produce, right now, a single list of every identity with standing access to your most critical systems, including the ones nobody remembers granting?

If that takes more than one query across more than one system, you've found your fragmentation problem.

2 Entitlement Sprawl: When Identity Growth Outpaces Governance Capacity

Most access-related risk is not created in a single decision. It accumulates over time. Every new role, project assignment, contractor engagement, SaaS deployment, acquisition, and business exception creates new permissions that rarely ever get reversed. Over time, these permissions accumulate into a growing inventory of latent entitlements, i.e., access rights that remain active long after their original business justification has disappeared.

The March 2026 attack targeting **Stryker Corporation**, a global medical technology firm, demonstrated the destructive potential of ungoverned elevated privileges in cloud environments. The attack saw Iranian state actors obtain administrative access through Stryker's Microsoft Entra ID deployment, then use Microsoft Intune to initiate mass factory resets, wiping Stryker's mission-critical devices and **triggering downtime across 79 countries.**

The underlying problem in this incident was slow and incomplete entitlement governance that could not keep pace with modern identity growth. Governance teams cannot continue tracking entitlements through periodic reviews when today's environments demand continuous visibility, graph-based relationship mapping, and automated lifecycle governance.

Pro tip:

Pull every entitlement that hasn't been touched, reviewed, or exercised in 90 days. You don't need a full audit to start. That single stale-access report is usually enough to reveal how much of your entitlement inventory is dead weight.

3 Manual Oversight Processes Cannot Keep Pace with Automation

Manual **identity governance and administration (IGA)** processes are slow, error-prone, and hard to scale. Yet many organizations still rely on them, using spreadsheets, ticket queues, and periodic certification campaigns to determine who has access and whether that access remains appropriate.

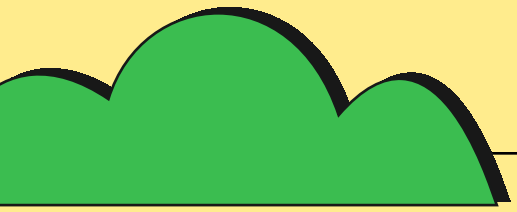
The challenge is that manual governance is strongest at the point where access is granted and weakest everywhere after. Permissions given to joiners, movers, leavers, contractors, and project-based identities, as well as temporary access requests, require continuous tracking and review. Manual processes cannot power this.

Ponemon found that **45% of internal identities and 34% of third-party identities** possess more access than necessary to perform their jobs. **Microsoft's 2024 Midnight Blizzard intrusion** demonstrated how dangerous this oversight can become. Attackers initially gained access by password spraying a legacy, non-production tenant that sat outside normal governance focus.

Beyond proving that governance gaps can emerge even in seemingly mature environments, relying on manual oversight in environments increasingly defined by automation, machine identities, and AI-enabled workflows is nothing short of self-sabotage....

Pro tip:

Ask your next certification campaign owner one question: "Would you personally vouch for every approval on this list, or are some of these rubber-stamped?" Their answer will tell you exactly where manual review has quietly stopped being any form of actual review.



4 Machine Identities Are Outpacing Human Identities, and So Is Their Risk

Organizations are overrun with machine identities and service accounts: APIs, bots, IoT devices, automation, signing keys, and, more recently, AI agents. According to 2026 CSA data, cloud-native environments contain **an average of 144 machine identities for every human identity**. Yet most identity governance programs remain overwhelmingly focused on workforce access.

This creates a dangerous asymmetry. Human identities follow some modicum of established onboarding, review, and offboarding processes. Machine identities, on the other hand, end up lacking clear ownership, lifecycle controls, entitlement oversight, and credential rotation policies. As a result, organizations can rarely tell exactly how many machine identities exist, whether they should still exist, what permissions they hold, who is accountable for them, and whether they are vulnerable.

The **Okta support-system breach** makes the stakes concrete. In this incident, attackers used a stolen access token and unrotated service account credentials to reach Cloudflare's Atlassian environment. Once inside, they specifically searched for secrets, tokens, remote access, and privileged infrastructure. Linx is out to change this. Our position is that as identity increasingly extends beyond people, governance must evolve from human-centric programs to **continuous, AI-driven access oversight.**

Questions to ask:

For your five most privileged service accounts, do you know who owns each one, when its credentials last rotated, and what would happen if you disabled it today? If any answer is "not sure," that account is a Cloudflare-style incident waiting for a trigger.

5 Growing Third-party Access Is Opening Up Unanticipated Gaps

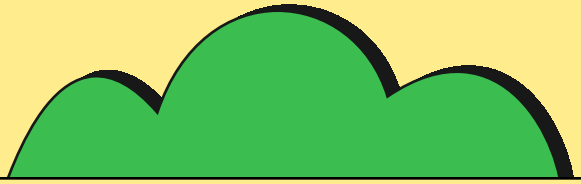
Modern enterprises increasingly depend on external identities. Contractors, consultants, managed service providers, suppliers, insurers, and software vendors now routinely access critical applications, infrastructure, and sensitive data.

Governance oversight typically declines as organizational dependency on third parties increases. Unlike employees, access by external identities is often provisioned through separate processes, managed by different stakeholders, and subject to inconsistent review cycles. The result is a growing population of high-impact identities that are difficult to inventory, monitor, and govern consistently.

This challenge is becoming increasingly visible in breach data. **Verizon's 2025 Data Breach Investigations Report** revealed that a third party was involved in **30%** of breaches, nearly double the previous year's figure. For CISOs, it is high time that external entities joined all other enterprise identities on one unified **identity graph** so that access and lifecycle decisions for all identities become evidence-backed.

Pro tip:

Cross-check your active vendor and contractor list against your active third-party access list. Any name that appears on one and not the other is either an offboarding gap or an access record nobody's maintaining; either way, it's worth chasing down.



6 Operationalizing Least Privilege at Enterprise Scale Remains Elusive

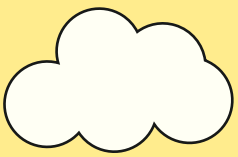
Few security principles enjoy broader support than least privilege. In theory, this means that identities should receive only the access required to perform their given tasks. In practice, however, maintaining least privilege across a modern enterprise is extraordinarily difficult.

Granting access is the easy part. The challenge is continuously aligning access decisions with changing business reality.

For example, **role-based access control (RBAC)** is a strong foundation, but how does a governance team know exactly what permissions people at different levels of finance, HR, procurement, and other departments need? When employees change roles or contractors move between projects, how does the governance team know to withdraw or adjust those permissions? For context, a 2026 report found that **70% of enterprises** have implemented **RBAC**, yet attacks tied to excess privilege abound.

More advanced least-privilege implementations, such as **attribute-based access control (ABAC)** and **Open Policy Agent (OPA)**, offer greater flexibility but introduce their own governance burden.

To resolve this, **mature governance programs** are turning to live access intelligence and entitlement analytics, visualized on context graphs built specifically to ensure access remains aligned with changing business needs.

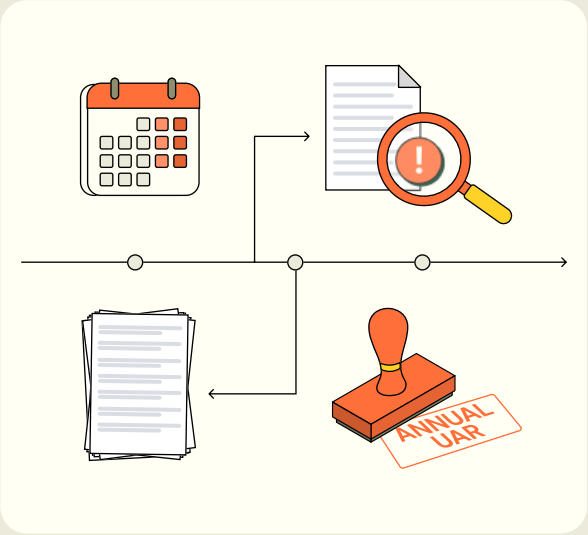


Questions to ask:

Pick any employee who changed roles in the last six months. Did their old permissions get withdrawn, or just supplemented with new ones? If you're not sure without checking, least privilege is merely a policy on paper, not a practice in production.

The Governance Maturity Map: How Mature Is Your IGA?

Evaluating where your enterprise sits on the governance maturity spectrum is the first step toward transforming identity from an operational bottleneck into a resilient, scalable control plane.



Level 1 Reactive

Manual/Compliance-Focused Governance

Governance is largely reactive and spreadsheet-driven. Access requests are generated manually via spreadsheets and come via IT tickets; reviews happen annually, just to check a compliance box.

Fragmented ownership means the same identity has different privileges in HR, Active Directory, and the cloud. Breaches are a matter of when, and non-compliance fines are sure to follow.

Data Anchors:

Spreadsheet-based review | Fragmented ownership

Level 2 Dashboard

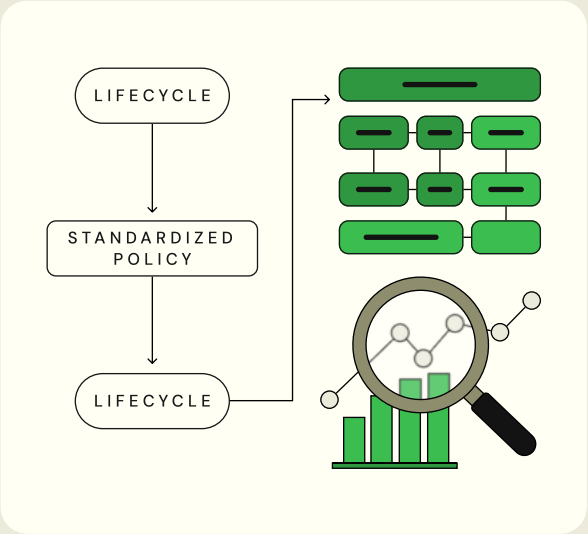
Visibility-Driven Governance

This level features automated discovery of identities and entitlements. Centralized dashboards show who has access to what, but governance is still episodic and triggered by audits.

Overprivileged orphaned accounts continue running until scheduled monitoring flags them. This may be good for reporting, but it proves weak for breach prevention.

Data Anchors:

Automated discovery | Episodic governance | Limited centralized reporting



Level 3 Lifecycle

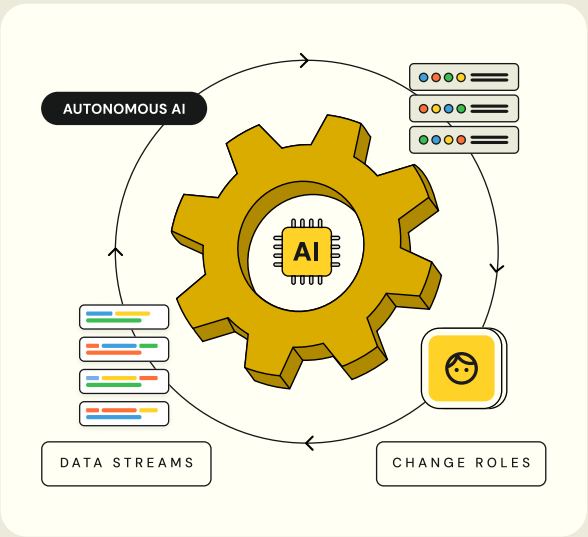
Intermediate, Risk-Informed Governance

This is where real control begins. Organization-wide policies are carefully created and standardized. A centralized solution ingests identity data from every IdP, normalizes *John Smith* versus *J-Smith* into a single source of truth, and enforces consistent entitlements.

Entitlement analytics help prioritize risk, and lifecycle controls flag permissions for review when something (e.g., a role, a vendor, or an NHI) changes.

Data Anchors:

- Unified Identity data normalization
- Continuous lifecycle control
- Entitlement analytics



Level 4 Continuous loop

Advanced, Adaptive Governance

Here, maturity reaches live, intelligent, context-aware identity and access modeling. Trust is evaluated continuously, even after login, based on adaptive cues like behavior, device, and location.

Governance decisions should happen autonomously, with role changes automatically triggering permission changes for movers (or revocations for leavers). A modern system oversees non-human identities and AI agents with the same rigor it applies to people. It continuously inventories service accounts and agentic identities, enforces just-in-time access and automated credential rotation in place of standing privileges, and scopes agent entitlements to the specific task at hand rather than the system they happen to run on.

User access reviews also change character at this level. Rather than routing a static spreadsheet to a manager who has to guess whether each line item is still justified, reviewers work with a tool that already understands the organization: its roles, its typical access patterns, and what "normal" looks like for a given identity. That context surfaces the entitlements that actually warrant a second look: the ones that deviate from peer group norms, sit unused, or were granted outside standard workflow. Certification becomes a targeted, evidence-backed exercise instead of a compliance ritual.

Data Anchors:

- Continuous adaptive trust evaluation
- Autonomous decision making (Movers/Leavers)
- Automated acess modeling

How Enterprises Benefit from a Mature Identity Governance Program

At maturity, identity governance is no longer merely a compliance exercise that erodes agility. It becomes a strategic control plane that reduces risk, supports Zero Trust initiatives, strengthens resilience, and scales security more effectively over time.

Outcome 1

Centralized Visibility Becomes a Given

Mature programs unify identity data from cloud, SaaS, on-premises, and hybrid systems into a single source of truth. By looking at one dashboard, CISOs can finally answer: Who has access, why, for how long, who approved it, when it should be revoked, and whether identities are acting in line with the permissions they were granted.

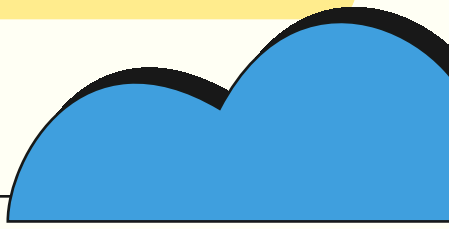
With this in place, access decisions are made intelligently, orphaned accounts are terminated immediately, overprivileged identities are automatically revoked, and compromised entities acting suspiciously are flagged in real time.

No more chasing spreadsheets or hunting through siloed **IAM** tools.

In practice

A contractor's Okta account is deactivated when their engagement ends, but a shadow admin account they created in a legacy on-prem tool six months earlier is never flagged because nobody is monitoring that system for orphaned identities.

In a mature program, that same dashboard shows both accounts, ties them to the same person, and closes both the moment the engagement ends, without a ticket ever being filed.



Outcome 2 Identity-Related Risk Drops Substantially

Visibility alone is not enough. True identity governance maturity will layer automated intelligence across three critical operational vectors to systematically shrink an organization's attack surface:

Active defense

Instead of static provisioning, CISOs are armed with complete ecosystem visibility to enforce tightly scoped permissions that automatically evaluate risk and revoke access when context changes, e.g. **JIT access**.

Preventative separation of duties (SoD)

Mature programs embed intelligent SoD directly into live workflows rather than relying on retroactive audits. The **Linx identity governance dashboard** automatically flags and blocks toxic permission combinations (e.g., creating a vendor *and* approving their payments) before they are ever granted.

Continuous certification

Mature governance replaces annual, checkbox-style compliance campaigns with context-aware, risk-centric **user access reviews (UARs)**. Reviewers receive evidence-backed analytics, eliminating blind rubber-stamping and accelerating threat detection.

In practice

A finance analyst requests vendor-management access for a one-off project. Under active defense, that access is granted as JIT and scoped to 14 days rather than standing indefinitely. When they later request invoice-approval rights on the same vendor, SoD logic catches the toxic combination and blocks it automatically, no audit finding required six months later.

At review time, their manager sees a risk-ranked summary instead of a 200-row spreadsheet, and actually reads it.

Outcome 3 Zero Trust Initiatives Become Truly Implementable

Zero Trust (never trust, always verify) depends on governance quality. Once governance matures, it acts as the source of truth for continuous trust evaluation. Instead of treating Zero Trust access as a one-time approval, the governance engine feeds real-time signals, role changes, risk scores, and behavior into policy decisions.

This enables contextual authentication before and beyond login, supports micro-segmentation, and limits blast radius, closing the gap between having Zero Trust policies on paper and actually enforcing them.

In practice

An engineer authenticates normally at 9 a.m. from their usual device and location. At 11 p.m. the same night, their credentials are used to access a source code repository from an unfamiliar IP. Because governance feeds live signals into the Zero Trust engine, that session is automatically stepped up for re-verification and the repository access is scoped down, rather than being treated as equally trusted just because the login succeeded.

Outcome 4 Non-Human Identities (NHIs) and Agents Stop Being Minefields

A mature governance program continuously inventories machine and service accounts. It then automatically adjusts access and permissions adaptively, enforcing autonomous credential rotation and just-in-time tokens rather than standing privileges.

For agentic AI, it manages ephemeral access, carefully calibrating agent entitlements to their job roles. In the **mature IGA that Linx champions,** forgotten service accounts with domain admin rights stop being a problem.

In practice

An AI agent is spun up to reconcile invoices against a purchasing system. Rather than being issued a standing API key with broad read/write access, it receives a short-lived token scoped only to the invoice tables it needs and which expires automatically when the task completes. When someone asks about what your AI agents "actually touch," the answer comes from the inventory, not from tracking down whoever configured the integration.

Outcome 5 Governance Maturity Boosts Operational Resilience

Mature identity governance programs reduce the likelihood and potential impact of identity-driven breaches, strengthening business resilience. They automatically enforce scoped permissions, which cuts privilege creep and effectively limits the attack blast radius.

They also eliminate manual processes where a single governance team must define permissions for hundreds of teams whose job roles they do not fully understand. Instead, self-service workflows replace those processes so that access requests and approvals are automated, intuitive, and policy-driven, cutting friction for business identities while retaining control with oversight teams.

Mature governance also provides the visibility and board-level accountability that regulators increasingly require. Across **GDPR**, **HIPAA**, **SOX**, **NIS2**, and **SEC** rules, attention is shifting from policy existence to control effectiveness. Mature programs are what produce the audit-ready evidence examiners want and the resilience to weather attacks.

In practice

A new hire on the procurement team needs access to a supplier portal. They don't file a ticket that sits in a queue for a governance analyst unfamiliar with procurement's workflows. Instead, they request it through a self-service portal that grants access automatically, scoped to exactly what their role requires. Three months later, their laptop is compromised via phishing. Because their access was scoped tightly instead of provisioned broadly "to be safe," the attacker inherits a narrow set of permissions instead of a wide one. The resulting incident stays contained to one supplier relationship instead of cascading across procurement. When the regulator asks for evidence of control effectiveness afterward, the access logs are the answer, not a scramble to reconstruct who approved what.

Outcome 6

Governance Itself Scales More Effectively Over Time

This is perhaps the most critical outcome for growth-stage enterprises. Over time, least-privilege implementation becomes fully automated for joiners, movers, leavers, contractors, and **NHIs**. AI-driven insights improve access recommendations, reducing entitlement sprawl. Workforce expansion, cloud workload growth, M&A integration, and AI adoption no longer trigger proportional administrative overload. Governance becomes a scalable asset, not a bottleneck.

In practice

An enterprise acquires a smaller company with its own identity provider, 200 employees, and a stack of unfamiliar SaaS tools. In an immature program, this means months of manual reconciliation and a temporary spike in risk while accounts get sorted out. In a mature program, the new identities are ingested into the same unified graph, mapped against existing role and entitlement models, and brought under governance in days, without the governance team growing headcount to match.

Achieving any of these outcomes does not entail a single leap. It requires organization-wide alignment.

Implementing a High-Level Strategy Across the Organization

Transforming identity governance from a tactical compliance chore into a strategic control plane requires alignment across leadership, operations, and the boardroom.

What this means for you (the CISO)

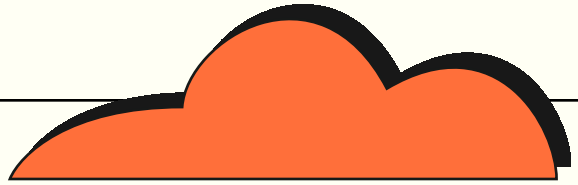
Your role shifts from managing access tools to overseeing a fundamental business resilience capability. Maturity gives you the data-driven clarity needed to measure risk, eliminate architectural blind spots, and prove control effectiveness across complex, multi-cloud environments.

What this means for your security team

Manual review fatigue, spreadsheet-driven audits, and reactive offboarding ticket queues disappear. Your team moves from administrative maintenance to proactive risk management, leveraging automated intelligence to flag toxic combinations and anomalous non-human identity behavior in real time.

Framing the boardroom conversation

When presenting to the board, move away from tool counts, licensing costs, and feature matrices. Instead, frame identity governance around **operational risk reduction, breach blast-radius containment, and business continuity.**



Evaluating Your Governance Posture: 6 Questions Every CISO Should Ask Today

For years, identity security maturity was measured through deployment milestones: **Zero Trust**, **MFA**, **SSO**, **PAM**. Those controls remain essential, but they no longer answer the questions that determine whether an organization can manage risk at scale.

Before presenting identity governance strategy to your board or executive leadership team, use these six operational diagnostic questions to assess your current exposure and maturity:

01 Visibility & integration coverage:

What percentage of our total application estate (SaaS, cloud, and legacy) is connected to a central platform for real-time entitlement visibility, and what resides in our unmonitored blind spots?

02 Non-human identity governance:

Do we have a complete, continuously updated inventory of service accounts, API keys, and AI agents, including explicit human owners, lifecycle end dates, and entitlement limits for every non-human entity?

03 Continuous authorization vs. authentication:

When an employee changes roles or a contractor project concludes, does access right-sizing occur automatically, or do we rely on periodic, manual certification campaigns to strip stale permissions?

04 Toxic combinations & separation of duties:

Can our current governance engine proactively detect and block toxic permission combinations (e.g., creating a vendor and approving payments) across multi-cloud environments before they are granted?

05 Least privilege at scale:

What proportion of our workforce currently holds active entitlements they have not used in the past 90 days, and how quickly can we identify and revoke that standing risk?

06 Audit & board readiness:

Can we immediately provide evidence-backed, graph-based proof of control effectiveness for GDPR, NIS2, or SEC compliance, or would an audit require manual spreadsheet aggregation across multiple teams?

Governance Maturity Is the New Measure of Identity Security and Operational Resilience

Identity governance has to evolve beyond compliance to become a continuous practice rather than a periodic exercise. Isolated controls are not enough; what organizations need is a unified understanding of how access, visibility, governance policy, and business operations interact across complex identity ecosystems.

Organizations that reach this level of governance maturity hold operational control, reduce risk, and build resilience against identity-based threats as complexity grows.

Partnering with Linx operationally actualizes advanced, adaptive governance (Level 4) that is continuous, contextual, and autonomous.