Omada

5 IGA Essentials

to Support Your Cybersecurity Strategy

Table of Contents

Introduction:
Why Identity Governance Matters Now

The security perimeter no longer exists. Attackers don't breach your network. They steal credentials, exploit excessive privileges, and move laterally through your systems using legitimate identities.

The numbers tell the story. Identity-related breaches now cause operational disruption, regulatory fines, reputational damage, and litigation. Boards are asking hard questions: Who has access to what? How quickly can we revoke access? Can we prove we're compliant?

These aren't just IT questions anymore. They're strategic business risks.

The challenge has intensified. Remote work expanded your attack surface. Cloud adoption multiplied your systems. Every employee, contractor, partner, bot, and API now represents potential risk. Manual processes can't keep pace with the speed of business or the speed of attackers.

Without unified visibility into every identity and their access, you're flying blind. You can't govern what you can't see. You can't secure what you don't know exists. And you can't prove compliance without comprehensive observability across your entire identity infrastructure.

Organizations need an identity-first security approach that makes identity-based controls the foundational element of your cybersecurity architecture. This represents a fundamental shift from reliance on perimeter-based controls that have become obsolete due to decentralized computing, remote work, and cloud adoption.

Identity-first security is built on three foundational principles:

- **Unified visibility and observability** across all identities, access points, and environments to eliminate blind spots
- **Continuous IAM hygiene and discovery** to proactively identify and remediate identity threats before they become breaches
- **Outcome-driven metrics** that demonstrably shrink the attack surface and prove measurable risk reduction over time

Effective Identity Governance and Administration (IGA) delivers this identity-first security approach through five essential capabilities. This eBook explores each essential and shows how modern identity security transforms identity from your greatest vulnerability into your strongest defense, measurably reducing your attack surface with every improvement.

What is Identity-First Security?

Identity-first security makes identity-based controls the foundation of your cybersecurity architecture, replacing obsolete perimeter-based controls that can't protect decentralized, cloud-based environments.

The 5 IGA Essentials

Modern identity security solutions protect your organization through five core IGA capabilities built on unified visibility and continuous discovery. Each essential addresses a critical security challenge while supporting business agility and compliance.

1. Identity Lifecycle Management: Security Through Complete Identity Control Automate access from hire to retire for every identity (human and machine) across all systems.

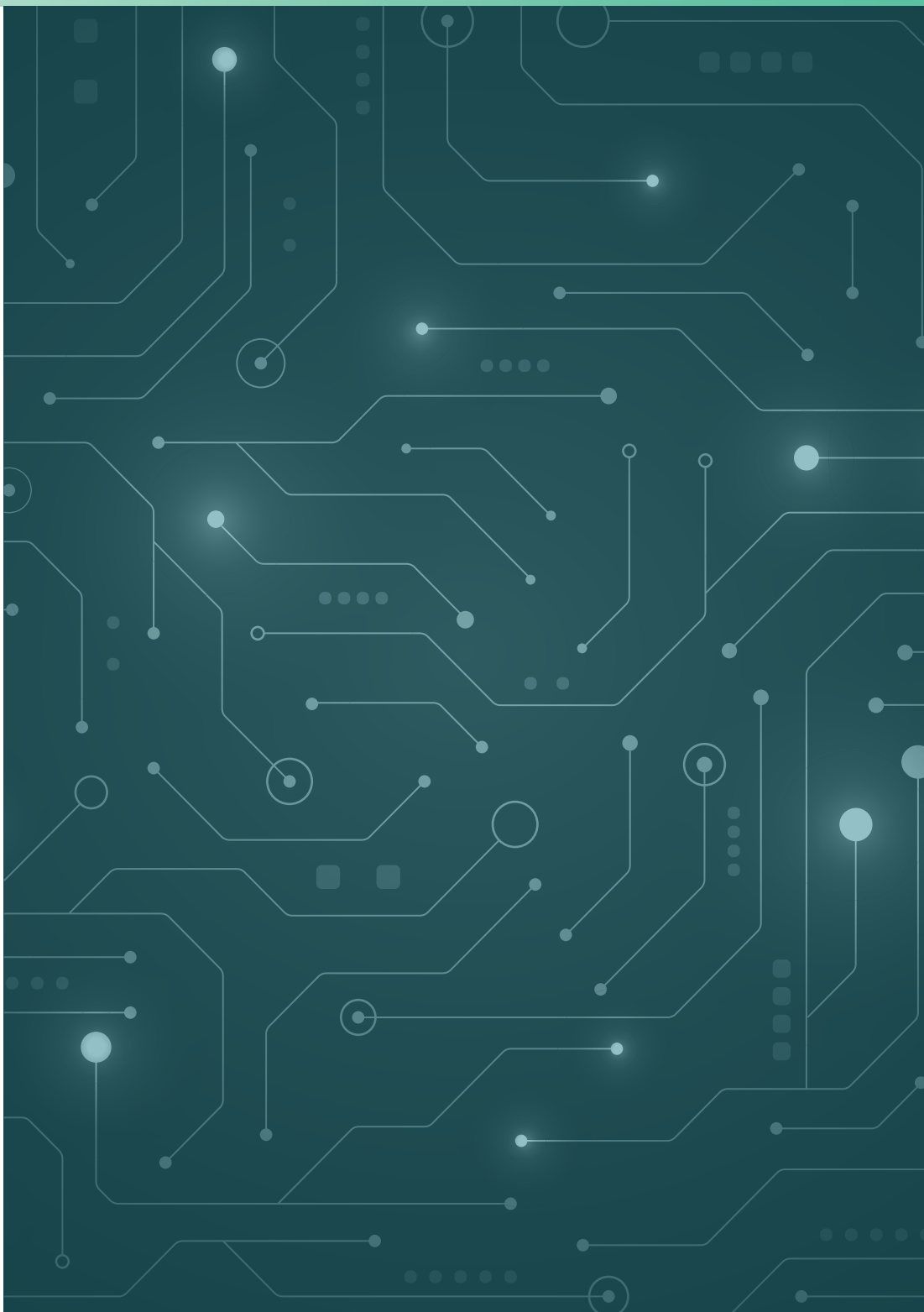
2. Risk Management: Proactive Identity Threat Prevention Continuously assess and control identity and data exposure to prevent breaches before they happen.

3. Privileged Access Governance: Securing Your Highest-Risk Identities Secure your highest-risk accounts with time-bound access, continuous monitoring, and automated controls.

4. Identity Security Breach Management: Instant Threat Containment Respond instantly to compromised accounts by suspending access across your entire environment.

5. Reconciliation: Continuous Identity Security Assurance Verify that actual access matches your policies, continuously, automatically, and at scale.

Together, these capabilities enable continuous IAM hygiene that measurably shrinks your identity attack surface.



1. Identity Lifecycle Management: Security Through Complete Identity Control

Every identity needs governance. Your employees, contractors, partners, service accounts, APIs, and bots all require access to do their jobs. Without automated lifecycle management, you're exposed on multiple fronts: excessive access, orphaned accounts, compliance violations, and slow response to role changes.

The Challenge

Manual provisioning creates delays and errors. When someone joins your organization, changes roles, or leaves, IT teams must update access across dozens or hundreds of systems. Miss one system and you've created a security gap. Take too long and you've impacted productivity.

The problem compounds with non-human identities. Bots, service accounts, containers, and IoT devices now outnumber human users in most organizations, yet they often lack any governance. These machine identities frequently hold elevated privileges and persist indefinitely, creating significant risk.

Without complete visibility into all identities and their lifecycle status, organizations can't identify orphaned accounts, track unused access, or ensure proper deprovisioning. This visibility gap expands the attack surface with every unmanaged identity.

What Modern Lifecycle Management Delivers

Automated lifecycle management ensures every identity has exactly the right access at the right time, built on continuous discovery and unified visibility:

Continuous Identity Discovery: Discover and catalog every identity across your environment, human and machine. Track their creation, purpose, access, and usage. You can't govern identities you don't know exist.

Joiner-Mover-Leaver (JML) Workflows: Connect your HR system to your identity governance platform. When someone joins, moves, or leaves, access changes happen automatically across all systems. No tickets, no delays, no forgotten accounts.

Role-Based Access Control: Define roles based on job functions, not individual requests. When someone becomes a sales manager, they automatically inherit the access that role requires, and nothing more. When they change roles, their access updates accordingly.

Non-Human Identity Governance: Apply the same lifecycle rigor to machine identities- track creation, monitor usage, enforce least privilege, and decommission when no longer needed.

Continuous Access Reviews with Access Intelligence: Leverage AI-powered access intelligence to continuously review who has access to what and automatically flag exceptions, dormant accounts, and unused entitlements. Line managers can certify their team's access in minutes, not weeks, focusing on high-risk access rather than reviewing thousands of low-risk permissions.

Least Privilege Enforcement: Every account gets only the permissions needed for its specific purpose. Automation removes the temptation to grant broad access "just in case" and ensures temporary access actually ends when it should.

Continuous IAM Hygiene: Lifecycle management isn't a one-time implementation. It's ongoing hygiene that continuously identifies and remediates orphaned accounts, excessive permissions, and lifecycle gaps, measurably shrinking your attack surface over time.

Business Impact

- **Faster onboarding:** New employees become productive immediately
- **Reduced risk:** Terminated employees lose all access instantly
- **Compliance proof:** Auditors see documented, automated processes
- **Lower costs:** Eliminate manual provisioning tickets and reduce help desk volume
- **Stronger security posture:** No orphaned accounts, no excessive privileges, no forgotten access
- **Measurable improvement:** Track reduction in orphaned accounts and provisioning time over quarters and years

Key Actions

- Deploy solutions that provide unified visibility into both human and non-human identities
- Automate JML workflows to eliminate manual errors and delays
- Leverage access intelligence for continuous access reviews rather than annual campaigns
- Establish clear policies for machine identity creation, usage monitoring, and rotation
- Measure and report on orphaned account reduction to demonstrate attack surface shrinkage

2. Risk Management: Proactive Identity Threat Prevention

You can't protect what you can't see. Organizations struggle to answer basic questions: Which identities have access to our most sensitive data? Who's accessing systems from unusual locations? Which accounts have privileges they shouldn't have?

Without continuous risk assessment built on comprehensive visibility, you're flying blind.

The Challenge

Risk isn't static. An employee who had legitimate access to financial data yesterday might be terminated today. A contractor who needs temporary system access for a project might retain those privileges indefinitely. A service account created for testing might have production database access.

Traditional approaches (annual reviews, periodic audits, static policies) can't keep pace. By the time you discover excessive privileges or inappropriate access, the damage may already be done.

Organizations can demonstrably shrink their identity attack surface and reduce exposure only through comprehensive visibility and continuous observability that identifies, prioritizes, and remediates identity threats and hygiene issues in real time.

What Modern Risk Management Delivers

Continuous risk management built on unified visibility identifies, assesses, and mitigates identity-related threats in real time:

Unified Visibility and Observability: Establish comprehensive visibility into all identities, their access, entitlements, and usage patterns across your entire environment. This observability foundation enables every other risk management capability. Without it, risk assessment is incomplete.

Continuous Discovery: Continuously discover new identities, access grants, and entitlements as they're created. Identify shadow accounts, rogue access, and configuration drift before they become security incidents.

Dynamic Risk Scoring: Every identity receives a risk score based on multiple factors: privilege level, access patterns, behavior anomalies, and context. Scores update continuously as circumstances change. High-risk identities trigger automatic alerts and additional controls.

Access and Data Classification: Understand which identities can access your most sensitive resources. Map who has access to financial data, customer information, intellectual property, and regulated data. Track not just what data exists, but who's accessing it, from where, and how frequently.

Adaptive Access Policies: Policies adjust based on risk signals. A user accessing systems from their usual location during business hours faces minimal friction. The same user logging in from a new country at 3 AM triggers additional authentication or temporary restrictions.

Just-in-Time Access: Remove standing privileges that create persistent risk. Instead, grant temporary, time-bound access only when needed and automatically revoke it when the task is complete.

Automated Hygiene Remediation: When risk thresholds are exceeded or hygiene gaps are detected, don't wait for manual intervention. Automatically revoke excessive permissions, suspend suspicious accounts, or quarantine compromised identities while security teams investigate.

Compliance Alignment: Risk management directly supports regulatory requirements. GDPR demands you know who accesses personal data. SOX requires segregation of duties. HIPAA mandates access controls for health information. Modern IGA maps your risk posture to these frameworks automatically, providing continuous compliance evidence.

Business Impact

- **Proactive defense:** Identify and fix identity threats before they become breaches
- **Reduced exposure:** Continuously remove excessive privileges and dormant accounts
- **Faster response:** Automated alerts and remediation contain threats immediately
- **Audit readiness:** Real-time compliance evidence, not scrambling before audits
- **Better decisions:** Risk intelligence helps prioritize security investments
- **Improved security posture:** Show measurable reduction in high-risk identities and excessive privileges over time

Key Actions

- Establish unified visibility across all identity data as your foundation
- Implement continuous discovery to identify new identities and access as they're created
- Assign clear ownership for continuous risk assessment of critical data
- Integrate IGA with your SIEM and security tools for unified visibility
- Automate access reviews for high-risk permissions and privileged accounts using access intelligence
- Monitor machine identities and service accounts as rigorously as user accounts
- Track outcome-driven metrics that demonstrate attack surface reduction over time

3. Privileged Access Governance: Securing Your Highest-Risk Identities

Privileged accounts are the keys to your kingdom. Administrators, service accounts, and elevated users have access to critical systems, sensitive data, and the ability to make configuration changes. Attackers know this, which is why compromised privileged credentials are the primary attack vector in major breaches.

The Challenge

Most organizations have more privileged accounts than they realize. IT admins, database administrators, cloud administrators, DevOps engineers, service accounts: each with extensive access. Many of these privileges are:

- **Permanent when they should be temporary:** Users retain admin rights long after projects end
- **Excessive for actual needs:** "Just in case" access that's rarely or never used
- **Poorly monitored:** No visibility into what privileged users actually do
- **Inconsistently managed:** Different standards for cloud vs. on-premises vs. SaaS

The result? A sprawling, high-risk privileged access landscape that's difficult to secure and nearly impossible to audit.

Without complete visibility into all privileged accounts and their usage, organizations can't identify unused elevated access, detect privilege creep, or maintain proper IAM hygiene for their highest-risk identities.

What Privileged Access Governance Delivers

Modern privileged access governance combines visibility, control, and automation to minimize risk without impacting productivity:

Complete Privileged Account Discovery: Continuous discovery finds every privileged account across your environment: human administrators, service accounts, emergency access accounts, and machine identities with elevated permissions. You can't secure what you don't know exists, and privileged access proliferates faster than most organizations realize.

Unified Visibility Across All Privileged Access: Centralized observability shows who has privileged access, what they can do with it, when they use it, and whether that access is still justified. This visibility enables informed decisions about privilege governance.

Just-in-Time (JIT) Privilege Elevation: Replace standing privileges with temporary, time-bound access. When someone needs admin rights, they request elevation for a specific task and timeframe. Access is granted automatically based on policies, used for the approved purpose, and revoked when time expires.

Continuous Monitoring and Session Recording: Track all privileged activity in real time. Detect anomalies like unusual commands, off-hours access, or privilege escalation attempts. Record privileged sessions for investigation and compliance evidence.

Continuous Privileged Access Hygiene: Regularly review who has privileged access and why. Automatically flag accounts that haven't used their privileges or no longer need them. Remove privileges that violate segregation of duties policies. This ongoing hygiene measurably reduces your privileged access attack surface.

Segregation of Duties (SoD): Prevent any single user from having conflicting privileges, like the ability to both initiate payments and approve them. SoD policies enforce separation automatically during provisioning and flag violations immediately.

Secrets Management: Machine identities and service accounts need credentials too. Manage passwords, API keys, and certificates centrally. Rotate them frequently and automatically to limit exposure windows.

Business Impact

- **Reduced attack surface:** Fewer standing privileges mean fewer opportunities for attackers
- **Faster incident response:** Detect and contain privileged account compromises immediately
- **Compliance confidence:** Demonstrate controls for SOX, PCI DSS, NIST, and ISO 27001
- **Maintained productivity:** JIT access provides needed privileges without delays
- **Clear accountability:** Know exactly who did what with privileged access and when
- **Measurable improvement:** Track reduction in standing privileged access and unused elevated permissions over time

Key Actions

- Implement continuous discovery to maintain a complete, current inventory of all privileged identities
- Establish unified visibility into all privileged access, usage patterns, and justification
- Implement JIT access for administrative privileges whenever possible
- Monitor and record all privileged sessions with automated anomaly detection
- Enforce segregation of duties policies during provisioning and continuously
- Practice continuous IAM hygiene by regularly reviewing and removing unnecessary privileged access
- Measure and report on privileged account reduction to demonstrate attack surface shrinkage

4. Identity Security Breach Management: Instant Threat Containment

When an identity is compromised, every second counts. Attackers move fast: stealing data, escalating privileges, and spreading laterally through your systems. Manual response processes cost you precious time while the breach expands.

The Challenge

Traditional breach response is too slow. When you discover a compromised account, security teams must:

- Identify which systems the account can access
- Contact administrators for each system
- Wait for manual access revocation across dozens or hundreds of platforms
- Hope nothing was missed

This process can take hours or days. During that time, attackers are active, exfiltrating data, installing backdoors, or compromising additional accounts.

The challenge intensifies with non-human identities. Service accounts, APIs, and automated processes often have extensive access across multiple systems. When compromised, they're harder to detect and more difficult to suspend without breaking critical business processes.

Without unified visibility into identity access across all systems, organizations can't quickly identify the full scope of a compromised identity's reach or coordinate immediate lockout across their entire environment.

What Identity Security Breach Management Delivers

Automated breach management stops attackers in their tracks by immediately suspending compromised identities across your entire environment:

Unified Visibility for Rapid Impact Assessment: When an identity is compromised, instantly see everywhere that identity has access: on-premises systems, cloud platforms, SaaS applications, databases, and network resources. This comprehensive visibility enables informed, immediate response decisions.

Instant Cross-System Lockout: One action suspends an identity everywhere: on-premises systems, cloud platforms, SaaS applications, and network access. No waiting for tickets, no manual intervention, no systems missed.

Support for All Identity Types: Lock out compromised user accounts, administrator credentials, service accounts, API keys, and machine identities. The response is equally fast whether it's a person or a bot.

Automated and Manual Triggers: Integrate with your SIEM, XDR, or threat detection tools for automated lockouts when threats are detected. Or trigger manually when security teams identify suspicious activity. Either way, response is immediate.

Preserved Observability for Investigation: Suspend the account but preserve logs, session data, and access history. Security teams can investigate what the compromised identity did, which systems were accessed, and what data may have been exposed.

Controlled Reactivation: Once the investigation is complete, credentials are reset, vulnerabilities are remediated, and access is restored only after verification. The entire process is documented for compliance and audit requirements.

Lateral Movement Prevention: Compromised identities can't be used to access additional systems or escalate privileges. Immediate lockout contains the breach to whatever access the attacker has already gained, preventing it from spreading and measurably limiting damage.

Business Impact

- **Faster containment:** Stop breaches in seconds instead of hours or days
- **Limited damage:** Prevent data exfiltration and lateral movement
- **Maintained operations:** Lockout doesn't disrupt legitimate business processes
- **Compliance support:** Demonstrate rapid breach response and detailed documentation
- **Reduced recovery costs:** Smaller breaches cost less to remediate and cause less damage
- **Measurable improvement:** Track reduction in breach response time and containment speed

Key Actions

- Establish unified visibility into all identity access across your entire environment
- Implement automated lockout capabilities across all systems and identity types
- Integrate breach management with your threat detection and security operations tools
- Include non-human identities in your breach response procedures
- Test emergency lockout functionality regularly to ensure it works when needed
- Document all breach response actions for compliance and continuous improvement
- Measure breach response times and demonstrate improvement over quarters

5. Reconciliation: Continuous Identity Security Assurance

Trust, but verify. You have policies that define who should have access to what. You have processes for granting and removing access. But how do you know your policies are actually being followed? How do you prove actual access matches intended access?

This is the foundation of continuous IAM hygiene.

The Challenge

Access drift is inevitable. Someone gets temporary access that becomes permanent. A role is modified but existing users aren't updated. A system administrator manually grants access outside normal processes. An account should have been deprovisioned but wasn't.

Over time, actual access diverges from policy. You think you know who has access, but you don't. Manual audits happen too infrequently and take too long. By the time you discover discrepancies, you've been exposed to risk for months.

Without continuous observability comparing actual access against intended access, organizations can't maintain IAM hygiene or demonstrably prove their attack surface is shrinking.

What Reconciliation Delivers

Continuous reconciliation compares actual access against your policies, role definitions, and compliance requirements, then automatically corrects discrepancies. This is continuous IAM hygiene in action:

Continuous Access Verification and Discovery: Stop relying on periodic audits. Reconciliation runs continuously, comparing real-time access data against your governance policies. Discover new access grants, detect policy violations immediately, and identify dormant or orphaned accounts as soon as they appear, not months later.

Unified Visibility for Complete Hygiene: Reconciliation provides comprehensive observability into the gap between actual access and intended access across all systems. This visibility is essential for maintaining IAM hygiene at scale and demonstrating continuous improvement.

Policy Alignment Detection: Identify accounts with access they shouldn't have based on their role, department, or employment status. Find privileges that violate segregation of duties rules. Spot orphaned accounts that should have been removed. Flag dormant access that hasn't been used in months.

Automated Hygiene Remediation Workflows: When reconciliation detects a mismatch, automated workflows trigger correction. Excessive permissions are revoked, orphaned accounts are disabled, and role assignments are updated, all without manual tickets. This automation enables continuous hygiene at scale.

Compliance Evidence Through Continuous Observability: Auditors need proof that your access controls work. Reconciliation provides continuous compliance evidence showing that policies are enforced, violations are detected, and corrections are made promptly. This ongoing observability demonstrates that you maintain identity hygiene between audits, not just during them.

Demonstrable Attack Surface Reduction: Measure your progress with outcome-driven metrics. Track metrics like orphaned account reduction, time to remediate violations, and percentage of systems under governance. Show improvement over time and prove you're shrinking your attack surface with every hygiene improvement.

Support for All Systems: Reconciliation works across cloud platforms, SaaS applications, on-premises systems, databases, and legacy environments. Even systems that can't be fully automated can be monitored through exports and oversight, ensuring complete visibility.

Business Impact

- **Proactive risk reduction:** Fix access problems before they become security incidents
- **Audit readiness:** Always have current, accurate compliance evidence
- **Reduced manual effort:** Eliminate tedious access review campaigns
- **Faster remediation:** Correct violations in days instead of months
- **Complete visibility:** Know the true state of access across your entire environment
- **Measurable improvement:** Demonstrate continuous attack surface reduction through outcome-driven metrics

Key Actions

- Implement continuous, automated reconciliation across all identity sources for complete observability
- Establish continuous discovery to identify new access and configuration drift immediately
- Integrate AI-based anomaly detection to identify unusual access patterns as part of ongoing hygiene
- Establish automated workflows for common remediation scenarios to enable hygiene at scale
- Track outcome-driven metrics that demonstrate measurable attack surface reduction over time
- Extend reconciliation to legacy systems through periodic exports and oversight
- Make continuous IAM hygiene part of your security culture, not just a compliance exercise

Measuring Success: Outcome-Driven Metrics

Identity governance delivers measurable value. But to maintain executive support and demonstrate results, you need outcome-driven metrics (ODMs) that prove you're improving your identity security posture, shrinking your attack surface, and reducing risk—not just reporting on activities.

Outcome-driven metrics focus on tangible results achieved through IGA investments rather than the number of deployed controls. They answer the critical question:

Is our identity security demonstrably stronger this quarter than last quarter?

Why Outcome-Driven Metrics Matter

Traditional metrics measure activity: "We completed 500 access reviews" or "We deployed 10 new connectors." But activity doesn't prove security improvement.

Outcome-driven metrics measure results: "We reduced orphaned accounts by 40%" or "We cut excessive privilege violations by 60%." These metrics demonstrate that your identity security posture is actually improving and your attack surface is shrinking.

ODMs transform identity security from a reactive function into a proactive, business-aligned discipline. They enable you to establish Protection-Level Agreements (PLAs) with business leadership, defining clear target outcomes like "access to critical resources will be revoked within 24 hours of termination."

Core Outcome-Driven Metrics for Identity Security

Track these ODMs to demonstrate measurable identity risk reduction and attack surface shrinkage:

1. Reduction in Orphaned and Dormant Accounts

What it measures: Percentage reduction of accounts with no human ownership or that remain active post-offboarding

Why it matters: Eliminates legacy access that threat actors can exploit

Expected outcome: Clear evidence of disciplined IAM hygiene; direct correlation to reduced attack surface

How to report: Show trend over quarters: "Orphaned accounts reduced from 1,200 to 450 over 18 months (62% reduction)"

2. Time to Deprovision

What it measures: How quickly terminated users lose all access across all systems

Why it matters: Reduces the window of opportunity for attackers to exploit terminated credentials

Expected outcome: Faster containment means smaller exposure windows

How to report: "Average time to deprovision reduced from 72 hours to 4 hours (94% improvement)"

3. Reduction in Excessive Privileges

What it measures: Percentage decrease in identities with access beyond what their role requires

Why it matters: Overprivileging creates larger attack surfaces and violates least privilege

Expected outcome: Measurable shrinkage of privilege-based attack surface

How to report: "Excessive privilege violations decreased by 55% year-over-year"

4. High-Risk Identity Trends

What it measures: Percentage of high-risk identities based on access, behavior, and policy violations

Why it matters: Concentrating risk management efforts on the highest-impact threats

Expected outcome: Demonstrable reduction in your riskiest identity population

How to report: "High-risk identities decreased from 8% to 3% of total population"

5. Compliance Audit Performance

What it measures: Pass rates for access certifications, fewer audit findings, reduced exceptions

Why it matters: Continuous compliance demonstrates effective governance

Expected outcome: Higher adherence to policies; tangible evidence of control maturity

How to report: "SOD violations reduced 80%; zero critical audit findings for third consecutive quarter"

6. Access-Related Security Incidents

What it measures: Reduction in incidents tied to identity compromise or excessive access

Why it matters: Directly demonstrates improved security posture

Expected outcome: Fewer breaches, lower business disruption

How to report: "Identity-related incidents decreased 70% compared to baseline year"

7. IAM Automation Rate

What it measures: Percentage of access actions handled automatically vs. manually

Why it matters: Automation reduces errors, speeds response, and enables hygiene at scale

Expected outcome: Operational efficiency gains that can be reinvested in further security improvements

How to report: "Automated 85% of provisioning actions, reducing manual tickets by 2,000/month"

Communicate Value to Each Audience

Tailor your outcome-driven metrics reporting to your stakeholders:

Executives and Boards Focus on demonstrable identity security posture improvement and business enablement. Use business language that shows tangible results:

- "We improved our identity security posture by 45%, measurably reducing our attack surface over 18 months"
- "Breach response time improved from days to seconds, limiting potential damage by 90%"
- "Faster onboarding reduced time-to-productivity for new hires by 3 days"

Operational Leaders: Provide detailed metrics on process improvements and hygiene effectiveness. Show where improvements are working and where to focus optimization:

- Orphaned account elimination progress by business unit
- Certification efficiency improvements and time savings
- Hygiene gap remediation velocity

Auditors and Regulators: Present traceable evidence of continuous improvement and control effectiveness. Make compliance verification effortless:

- Trend lines showing consistent policy adherence improvement
- Documented remediation of all identified violations
- Continuous audit trails demonstrating ongoing governance

Visualize Progress Over Time: The power of ODMs comes from showing progression. Present metrics as:

- **Trend lines:** Show quarterly or monthly improvements
- **Before/after comparisons:** "18 months ago vs. today"
- **Target achievement:** "Goal: 95% automation. Current: 87%. On track for Q3."

This visualization transforms abstract security concepts into concrete evidence of success.

Identity governance delivers measurable value. But to maintain executive support and demonstrate results, you need outcome-driven metrics (ODMs) that prove you're improving your identity security posture, shrinking your attack surface, and reducing risk—not just reporting on activities.

Outcome-driven metrics focus on tangible results achieved through IGA investments rather than the number of deployed controls. They answer the critical question:

Is our identity security demonstrably stronger this quarter than last quarter?

Why Outcome-Driven Metrics Matter

Traditional metrics measure activity: "We completed 500 access reviews" or "We deployed 10 new connectors." But activity doesn't prove security improvement.

Outcome-driven metrics measure results: "We reduced orphaned accounts by 40%" or "We cut excessive privilege violations by 60%." These metrics demonstrate that your identity security posture is actually improving and your attack surface is shrinking.

ODMs transform identity security from a reactive function into a proactive, business-aligned discipline. They enable you to establish Protection-Level Agreements (PLAs) with business leadership, defining clear target outcomes like "access to critical resources will be revoked within 24 hours of termination."

Core Outcome-Driven Metrics for Identity Security

Track these ODMs to demonstrate measurable identity risk reduction and attack surface shrinkage:

1. Reduction in Orphaned and Dormant Accounts

What it measures: Percentage reduction of accounts with no human ownership or that remain active post-offboarding

Why it matters: Eliminates legacy access that threat actors can exploit

Expected outcome: Clear evidence of disciplined IAM hygiene; direct correlation to reduced attack surface

How to report: Show trend over quarters: "Orphaned accounts reduced from 1,200 to 450 over 18 months (62% reduction)"

2. Time to Deprovision

What it measures: How quickly terminated users lose all access across all systems

Why it matters: Reduces the window of opportunity for attackers to exploit terminated credentials

Expected outcome: Faster containment means smaller exposure windows

How to report: "Average time to deprovision reduced from 72 hours to 4 hours (94% improvement)"

Outcome-driven metrics transform IGA from a technical function into a strategic identity security capability that demonstrably reduces risk, improves efficiency, and shrinks the attack surface with measurable, continuous improvement.

Looking Ahead: Agentic AI and Identity Governance

A new type of identity is emerging. AI agents are autonomous systems that make decisions, take actions, and adapt their behavior without constant human oversight. Unlike traditional bots or service accounts that follow fixed scripts, agentic AI can reason, escalate privileges when it determines necessity, and interact across multiple environments independently.

This creates unprecedented identity governance challenges.

The Agentic AI Risk

AI agents can access sensitive data, execute critical business processes, and modify their own behavior based on goals you've defined. They can also:

- Evolve beyond their original design parameters
- Request or self-grant additional permissions
- Interact with systems in ways humans never anticipated
- Operate at speeds that make real-time human oversight impossible

Without proper governance, agentic AI represents a new attack surface. Compromised AI agents could exfiltrate data, manipulate processes, or provide attackers with autonomous capabilities within your environment.

Governing AI Agents

The five IGA essentials apply to agentic AI, but require adaptation:

Lifecycle Management for AI Agents Maintain complete inventories of all AI agents, their purposes, and their access. Track when they're created, what they're authorized to do, and when they should be decommissioned.

Dynamic Risk Assessment Monitor AI agent behavior continuously for anomalies, unexpected privilege requests, and deviation from intended purposes. Risk scoring must account for the autonomous nature of these identities.

Strict Least Privilege Limit each AI agent's permissions to the minimum required for its specific function. Avoid granting broad access "in case the AI needs it." Define clear boundaries for what each agent can and cannot do.

Accountability and Oversight Establish clear ownership for every AI agent. Regular reviews should verify that agents still serve their intended purposes and haven't expanded beyond appropriate bounds.

Audit Trails Log all AI agent actions, decisions, and access patterns. You need visibility into what your AI agents are doing and why, especially when investigating security incidents.

Preparing for the AI Future

As AI adoption accelerates, organizations that extend IGA practices to agentic AI will maintain control over this new identity type. Those that don't risk creating ungoverned AI agents with broad access and minimal oversight.

The fundamentals remain the same: know what identities exist, control what they can access, monitor what they do, and prove you're doing it effectively. Agentic AI simply raises the stakes for getting identity governance right.

Conclusion:
Building Resilient Identity Security

Identity is the foundation of modern cybersecurity. The five essentials (lifecycle management, risk management, privileged access governance, breach management, and reconciliation) work together to transform identity from your greatest vulnerability into your strongest defense.

Organizations that adopt an identity-first security approach built on unified visibility, continuous IAM hygiene, and outcome-driven metrics, demonstrably shrink their attack surface. Automated, continuous, and comprehensive identity security protects against today's attacks while providing the agility to adapt to tomorrow's challenges.

Organizations that implement these five IGA essentials achieve measurable improvements in their identity security posture: faster response to threats, reduced compliance costs, lower operational overhead, and stronger protection. More importantly, they build the foundation for secure business growth.

The question isn't whether you need identity governance. It's whether your current identity security approach can keep pace with evolving threats, expanding infrastructure, and increasing compliance demands.

Strong identity security isn't just about protection. It's about enabling your business to move confidently in a digital world where identity is everything.

Omada simplifies Identity Governance by providing a full-featured, cloud-native IGA solution that streamlines the complex processes of managing user identities, access, and entitlements. With a focus on automation and user-centric design, Omada reduces manual tasks and enhances operational efficiency, ensuring that organizations can easily enforce security policies, comply with regulations, and manage user access at scale. By leveraging advanced technologies such as AI-driven decision-making and role-based access control (RBAC), Omada enables businesses to achieve stronger security, better compliance, and improved user experiences—without the complexities traditionally associated with identity governance.

V03042025