Lumos

The 2025 Buyer's Guide to Modern Identity Governance & Administration

Executive Snapshot

Modern Identity Governance & Administration (IGA) is no longer just a compliance necessity; it's a strategic imperative for business resilience and growth. Selecting the right platform means moving beyond legacy limitations to achieve tangible outcomes across security, productivity, and cost savings. You don’t even have to completely replace your current IGA to achieve these outcomes. Solutions like Lumos let you augment your existing IGA with the power of agentic AI to auto-discover access, mine roles, build policies and surface any hidden access anomalies.

Problem: Legacy IGA fails in today's complex landscape (650+ apps avg., 50:1 machine-to-human identity ratio).

Solution: Modern IGA focused on automation, intelligence, and outcomes (Security, Productivity, Profitability).

Key Actions: Use toolkits (Sec 3), evaluate your criteria (Sec 4), ask critical questions (Sec 5), focus on ROI (Sec 6).

Goal: Select a unified platform governing all identities, delivering rapid TTV and measurable results.

This table summarizes the core business outcomes modern IGA delivers and typical benchmarks:

Outcome	Why It Matters	KPI Benchmarks*
Secure the Business	Fewer risks and smoother audits through continuous least-privilege governance.	40% faster reviews, 80% fewer standing privileged accounts[1]
Unlock Productivity	Employees productive on Day 1 and IT ticket queues shrink via zero-touch lifecycle automation.	90% cut in lifecycle effort; 40% fewer access tickets[1]
Increase Profitability	Frees budget by reclaiming unused licences and consolidating SaaS tools.	≥15% lower software costs[1]

Benchmarks aggregated from analyst surveys and modern AI-powered IGA deployments. [1] Source: Lumos customer data and industry reports.

How to use this guide:

Understand the market forces driving change (Section 2), then systematically work through Sections 3–15 to define requirements, establish evaluation criteria, compare vendors effectively, build a robust business case, and take action using the checklist in Section 16.

1 Why modern IGA is imperative

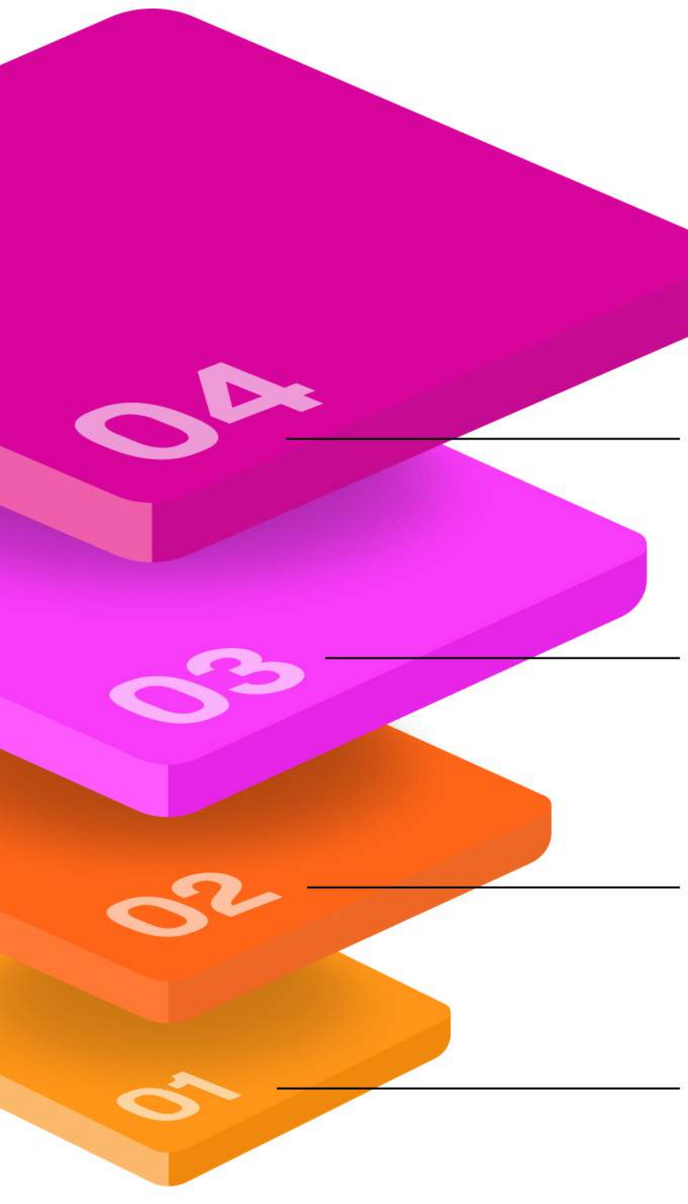
Legacy IGA tools—built for on-prem environments and human identities—can't keep pace with today's SaaS-heavy, non-human identity (NHI)-rich world. Understanding the shifts driving this imperative is the first step toward selecting the right solution for you.

Digital Shifts: The explosion of SaaS apps (650+ per enterprise), cloud adoption, a surge in machine identities (outnumbering humans 50:1), and hybrid work have drastically expanded the attack surface, data siloes and governance complexity.

Legacy Pain: Traditional IGA tools are slow (18+ month rollouts), brittle, and cover less than 20% of apps. Manual, spreadsheet-heavy processes create errors, delay audits, and frustrate users. Tools with visibility but no automation leave security gaps, while high TCO stems from complex upkeep and services.

Operational Scale: Today's IT and security teams are left reacting to changes in environment and threat landscape. Modern IGA must provide the scale and speed via autonomy. Evaluating tools on these four pillars of autonomous identity is essential: Perceive (visibility), Analyze (insights), Act (automation), and Learn (self-optimization).

Board Pressure: Boards now expect strong identity governance to ensure security, efficiency, and cost control, making IGA a top-level priority amid rising breach and audit risks.



Four key capabilities:

04: Learn
Adaptive Systems

03: Act
Full-Cycle Automation

02: Analyze
Actionable Insights

01: Perceive
Complete Visibility

Modern IGA platforms must address these challenges by:

- Governing both human and non-human identities.
- Automating identity lifecycles and access reviews.
- Delivering integrated visibility and automated action (not just alerts).
- Continuously adapting and improving through AI and machine learning.

Key Takeaway

Legacy IGA systems present significant challenges in handling modern digital complexity. Automation and intelligence, guided by a framework emphasizing visibility, analysis, action, and learning, are essential for security, efficiency, and meeting board-level expectations.

2 IGA 101 & market context

IGA manages the identity lifecycle and governs access across diverse environments. Understanding the core functions and market landscape is crucial before you evaluate vendors.

Key functional pillars include the following:

Visibility & Discovery: Inventorying every user (employee, contractor, partner), machine identity (service accounts, API keys, bots), application (managed and shadow IT), entitlement, group, and role. Correlating usage/activity data across hybrid environments.

Lifecycle Automation (JML): Orchestration of joiner, mover, and leaver events, integrating with any HRIS, IdPs and cloud providers, and automating fine-grained provisioning/deprovisioning workflows without manual IT tickets.

Access Requests & Fulfilment: Self-service portals (web AppStores, Slack/Teams integrations, ITSM/IaC integrations) for users to request access, governed by automated policy checks and approval workflows, including Just-in-Time (JIT) and Time-based access.

Access Reviews & Policy Enforcement: Periodic, event-driven, or continuous certification of access appropriateness, using risk context, usage data, and delta reporting (showing only changes) to streamline reviews. Includes remediation of violations like Separation of Duties (SoD), toxic combinations, etc.

Policy & Role Management: Definition, management, analysis, and optimization of access policies (role-based access control (RBAC), attribute-based access control (ABAC)). Modern solutions leverage AI/ML for role mining (suggesting roles based on usage) and policy recommendations.

Analytics & Reporting: Dashboards for identity risk posture, license usage, compliance status (SOX, SOC 2, ISO 27001, etc.), audit trails, operational efficiency, and AI-driven insights for optimization and risk reduction.

The market is moving towards an integrated "identity fabric" approach, where IGA acts as a central integration and orchestration layer.

Key Takeaway Modern IGA spans visibility, lifecycle automation, access requests, reviews, policy, and analytics, crucially covering both human and non-human identities across the entire IT landscape.

3 Preparation toolkit

A successful IGA selection project requires diligent preparation and cross-functional alignment. Avoid reactive, rushed decisions. Use these tools to build a solid foundation. Orient yourself and your stakeholders by using these tools to define scope, roles, and value.

Stakeholder RACI & "What's In It For Me?":
Clearly define roles (Responsible, Accountable, Consulted, Informed) for key project phases across Security (IAM, InfoSec), IT (Ops, Engineering, Architecture), HR, Finance (Procurement, SaaS Management), Compliance/Audit, and Line-of-Business Application Owners. Understand each group's primary motivations (for example, Security wants risk reduction, IT wants ticket reduction, Finance wants cost savings) and how the IGA project benefits them.

Environment Inventory Worksheet:
Document your current state to provide clear context to vendors and scope the project accurately. Include:

- Identity Sources: Primary IdP(s) (Okta, Entra ID), and other directories.
- HRIS: Workday, BambooHR, SAP SuccessFactors, etc.
- User Populations: Counts for Employees, Contractors, Partners, Customers (if applicable), and estimated NHIs - machines, service accounts, agents, etc.
- Critical Applications: Key SaaS (such as Salesforce, M365, Google Workspace, Workday, NetSuite), Cloud Platforms (AWS, Azure, GCP), On-Prem systems, and major Custom Applications. Note existing integration methods/challenges.
- Existing IAM/IT Tools: Current IGA (if any), PAM, ITSM (ServiceNow, Jira), CIEM, SIEM, Endpoint Security, and SaaS Management Platform (SMP).
- Connectivity Gaps: Identify systems lacking modern APIs (SCIM, REST) or requiring specialized integration. (Sample Row: App: AWS | Owner: Cloud Ops | Users: 200 Humans, 1500 Service Accts | Connector: Native API | Governance Need: IAM Role/Policy Review, JIT for Prod Access)

Value-Driver Canvas:
Explicitly map your specific project goals and compelling events (for example, upcoming SOX audit, recent M&A activity requiring integration, cut SaaS spend, improve onboarding experience) to the three core value drivers: **Secure the Business**, **Unlock Productivity**, and **Increase Profitability**. This keeps the focus on measurable business impact.

Discovery Question Bank:
Prepare targeted, open-ended questions for different stakeholders based on the value drivers to uncover deep-seated pain points and quantify potential benefits.

Key Takeaway

Thorough preparation involving stakeholder alignment, environment inventory, value mapping, and targeted questions is critical for a successful IGA selection.

4 Evaluation criteria & weights

Define your scoring criteria and assign weights based on your organization's priorities. This table provides sample criteria and weights emphasizing speed, automation, unification, and intelligence—hallmarks of a modern IGA approach. Weights below are illustrative; adjust them to reflect your own risk and cost drivers (for example, weight 'Compliance & Reporting' higher if facing an imminent audit).

Criterion	"Great" Looks Like	Sample Weight
Integration Depth & Speed	AI-assisted/low-code connector dev (< five days), 300+ OOTB deep integrations (CRUD + granular entitlements)	15%
Time-to-Value (TTV)	Demonstrable live pilot ≤ four weeks, minimal professional services required for core setup & key apps	12%
Unified IGA with Analytics	Single platform, data model, and connector set for identity governance, with advanced analytics and reporting.	10%
AI-Driven Insights	Explainable role-mining, risk scoring (user/entitlement), cost analysis, SoD detection, anomaly alerts	10%
Full-Cycle Automation	Robust, automated JML (incl. movers), JIT (request/grant/revoke), Delta UARs, Policy/SoD Enforcement	10%
User Experience & Zero-Touch IT	Intuitive self-service (Web, Slack/Teams, CLI), < five min automated approvals for policy-matched requests	8%
SaaS Spend Optimization	Automated license reclamation workflows, renewal alerts, app redundancy identification	7%
Non-Human ID Governance	Discovery, ownership, review, lifecycle mgmt (rotation, offboarding) for Service Accts, API Keys	7%
Compliance & Reporting	Auditor-ready evidence export, dashboard mapping to frameworks (SOX, SOC 2, GDPR, etc.), policy enforcement	6%
Scalability & Performance	Proven ability to handle large identity/app volumes without degradation, robust hybrid support	5%
Support & Partnership	Responsive support SLAs, proactive CSM, strong references, clear roadmap alignment	5%
Pricing & TCO	Transparent, predictable pricing, minimal PS dependency, clear ROI path	5%

5 Must-ask vendor questions

Move beyond standard RFP checklists during demos and Proofs of Concept (PoCs). Ask probing questions that reveal true capabilities, differentiate vendors, and validate claims about Time-to-Value (TTV) and automation effectiveness. (Aim for concise questions, focusing on the core validation needed).

Integration Speed & Depth

"Can you demonstrate building a new, functional, deep connector for one of our specific target apps live during the PoC, within five business days, using standard tools?"

WHY ASK?

Validates real-world integration speed vs. hidden PS dependencies and major TCO drivers.

Automation Effectiveness

"What percentage of access review items are typically auto-approved/rejected based solely on platform logic (delta, inactivity, risk) in customer deployments?"

WHY ASK?

Measures the real-world impact of intelligence in reducing manual review burden.

"Demonstrate a full 'Offboarding' workflow triggered by HRIS, showing automated access changes across systems resolved end-to-end in < five mins without manual IT steps."

WHY ASK?

Validates the depth, reliability, and speed of core lifecycle automation, a key productivity driver.

Time-to-Value & Cost Savings

"Provide the calendar days it took three recent, comparable customers to govern their first 15 apps."

WHY ASK?

Demands concrete proof of deployment velocity beyond marketing slogans.

"Provide verifiable examples of annual license cost savings achieved by three recent customers via your platform's automated reclamation workflows. What was the typical % saving?"

WHY ASK?

Tests tangible financial ROI delivered by unified IGA visibility and automation capabilities.

Machine Identity Coverage

"How does your platform discover, inventory, classify, and govern access for NHIs across cloud/on-prem? How is ownership assigned, reviewed, and lifecycle managed?"

WHY ASK?

Probes the maturity and completeness of governance for this critical identity type.

AI & Insights

"Build RBAC policy and explain the logic for your AI role mining or risk scoring. Show the 'explainability' feature. How can admins easily validate or override AI suggestions?"

WHY ASK?

Assesses policy management capability with the transparency, trustworthiness, and practical usability of AI features.

"Identify users with outlier access compared to their defined role or team peers."

WHY ASK?

Assess the depth of integration coverage and data fidelity that is used by AI for training the models.

Architecture & Hybrid Support

"How does your SaaS platform securely connect to and manage our on-premises systems?"

WHY ASK?

Validates the viability, security, and operational impact of hybrid connectivity at a high level.

> Gartner estimates that 50% of IGA deployments are in 'distress. "Organizations deploying IGA systems will continue to experience extended timelines due to incorrect use-case documentation, corrupted authoritative source identity data and misleading entitlement data"

Avoid These Top 5 Mistakes When Deploying IGA | Gartner®

6 Cost & ROI model

Justify your IGA investment with a clear business case focused on quantifiable value and a rapid return. Modern, unified platforms are designed to deliver significant ROI quickly, often achieving payback in under twelve months.

TOTAL COST OF OWNERSHIP (TCO)

Key Components:

Subscription/License Fees:

Understand the model clearly (per identity [human/machine], per application, platform tiers, bundled vs. à la carte features).

Implementation Services:

Factor in any required Professional Services (PS). **Modern SaaS aims for minimal PS** for core deployment due to OOTB (out-of-the-box) integrations and configuration wizards.

Internal Staff Time:

Estimate time for your team (IAM, IT, Security, App Owners) for deployment, configuration, ongoing administration, and maintenance. **Automation should significantly reduce this operational burden.**

Integration Costs:

This is a major differentiator. IGA might have a separate pricing model for integrations and custom connectors. **Modern platforms with large OOTB libraries and AI-assisted/low-code builders should have no additional cost.**

RETURN ON INVESTMENT (ROI)

Key Drivers:

Hard Savings:

- Reclaimed Unused Software Licenses: Quantify potential savings by identifying and deprovisioning inactive licenses.
- Consolidated Redundant Applications: Identify potential savings by eliminating overlapping tools.
- Reduced/Avoided Professional Services Costs: Compare minimal modern PS vs. extensive legacy PS costs.
- Potential Reduction in Cyber Insurance Premiums: Improved security posture may lead to lower premiums.

Efficiency Gains:

- Reduced IT Helpdesk Tickets: Estimate savings from fewer manual access requests/resets.
- Reduced Manual Effort for JML: Estimate time saved by IT/HR on lifecycle tasks.
- Reduced Manager/Admin Time on Access Reviews: Estimate time saved via automation/delta reviews.
- Faster Employee Onboarding / Time-to-Productivity: New hires get needed access on Day one.

Risk Reduction:

- Reduced Likelihood/Impact Cost of Breaches: Lower probability of identity-related incidents and associated costs.
- Reduced Cost of Audit Findings: Fewer findings, less remediation effort.
- Improved Compliance Posture: Avoiding potential regulatory penalties.

Simple ROI Formula:

[(Total Annual Savings - Annual TCO) / Annual TCO] * 100

Payback Period (Months) = (Total Year-1 Investment [License + Implementation]) / (Total Annual Savings / 12)

Use the drivers above to estimate your specific savings and calculate your potential ROI and payback period.
A payback of **less than twelve months** is a realistic target for modern, unified IGA platforms.

7 Common pitfalls and how to avoid them

Navigating the IGA market and implementation requires avoiding frequent missteps that can derail projects, inflate costs, and diminish value. Consider these common pitfalls and mitigation strategies:

Visibility Without Action

Tools that identify risks but lack automated remediation create manual work and leave gaps.

MITIGATION

Prioritize platforms that pair insights with automated actions

Treating SSO Bolt-Ons as IGA

Basic governance in AM tools lacks deep entitlement visibility and full lifecycle coverage.

MITIGATION

Ensure full-spectrum IGA—JML, NHI, analytics, and policy enforcement.

Lack of Unified Experience

Separate tools to manage IGA outcomes mean duplicate connectors, data silos, and higher costs.

MITIGATION

Use unified platforms with a shared data model and connectors.

Underestimating Integration Complexity

"Out-of-the-box" often means expensive PS for custom apps.

MITIGATION

Test integrations during PoC and ask for customer references.

Ignoring Other Types of Identities

Contractors tied to different HRIS systems and NHIs are often unmanaged and vulnerable.

MITIGATION

Look for built-in comprehensive lifecycle, ownership, and review capabilities.

Prioritizing Features Over Outcomes

Focusing on features without linking to business impact leads to poor results.

MITIGATION

Use tools like the Value-Driver Canvas to align with goals.

Poor Change Management and Adoption Strategy

Without training, communication, and stakeholder buy-in, adoption suffers.

MITIGATION

Build a change plan with exec sponsorship and training from the start.

Lack of Agentic AI Roadmap

Ensure purpose-built Agentic AI systems with outcome-driven initiatives rather than just an AI wrapper.

MITIGATION

Inspect AI architecture and see it in action for complete evaluation.

9 Augment, Don't Replace Your Existing IGA with Lumos

Modernizing your identity governance strategy doesn't always require a full rip-and-replace. If you're already using legacy or SaaS IGA platforms, Lumos can integrate directly into your existing environment; adding a powerful layer of agentic intelligence and analytics on top.

Extend your existing IGA investment with Lumos by unlocking:

Agentic Intelligence for Governance:
Albus, Lumos' identity AI agent, continuously analyzes HRIS, IdP, application, and usage data to recommend RBAC/ABAC policies, detect risky access, validate least privilege, and propose remediations. This isn't just insight — it's governance that thinks, reasons, and prepares actions for you.

Unified Access & Usage Visibility (Across All Identities):
Traditional IGAs rely on assignment data. Lumos goes deeper: real-time entitlement-level visibility, usage telemetry, peer baselines, NHI/service account analysis, and shadow IT discovery. You finally see what access actually does and where it's risky.

Accelerated Role Mining & Clean Policy Enforcement:
Legacy IGA role projects stall for months. Lumos automates the messy part: analyzing attributes, clustering users, mapping entitlements, and generating clean RBAC/ABAC drafts in hours. Push policies into other IGA platforms with one click or enforce them natively with Lumos IGA platform.

Agentic Access Reviews (UARs Done Right):
No more rubber-stamp campaigns. Lumos takes the first pass: flagging anomalies, validating usage, surfacing outliers, and recommending keep/remove actions. Approvers only review what truly matters, cutting review cycles from weeks to minutes.

Autonomous Anomaly Detection & Identity Threat Insight:
IGA tools show scores; Lumos finds the story. Detect SoD drift, dormant admin access, suspicious logins, privilege creep, and entitlement misuse. Lumos correlates privileges, identity context, and activity logs across systems, generating explainable risk narratives.

Natural-Language Identity Governance:
Ask questions like:

- "Which Snowflake admins haven't used their access in 90 days?"
- "Who owns this entitlement?"
- "What are the top identity risks across human + non-human identities?"

Lumos answers in plain English — with evidence, context, and recommended fixes.

Instant Time-to-Value:
You'll see actionable insights within 24 hours of connecting Lumos to your stack. No replacement, long deployments or custom projects required.

Think of Lumos as your identity co-worker: handling 80% of the tedious, repetitive governance work while your team focuses on strategy. You get a dynamic, intelligent, and flexible layer that transforms your IGA from reactive to autonomous; without losing what you've already built.

8 Start with or Augment Your IGA Platform

Choosing your next Identity Governance & Administration platform is a strategic investment—essential for securing your growing attack surface, increasing agility, and controlling SaaS costs. Legacy tools and fragmented solutions can't keep up. Success depends on platforms that drive value across three core areas - Security, Productivity and Profitability and here's how Lumos rises to the challenge:

Secure the Business

Shift from reactive compliance to proactive risk reduction with Lumos' full visibility, intelligent detection, and streamlined audits:

- Unified access visibility across SaaS, cloud, and on-prem
- **AI/ML-based risk detection** based on identity context and behavior
- Automated **access reviews** and certifications to cut prep time

Unlock Productivity

Automate identity lifecycle and access requests to eliminate manual work and free up IT and Security teams with Agentic AI.

- **Albus AI Agent** to auto-generate and enforce policies
- **Self-service access** requests via dynamic web store and Slack/Teams integrations
- **JML workflows** with automated provisioning/ de-provisioning

Increase Profitability

Take control of SaaS spend with real-time license and usage visibility and intelligent license management - all in one unified dashboard.

- **Unused license reclamation** and tier downgrade recommendations
- Usage tracking down to the entitlement level
- Consolidated view of contracts, costs, and renewals

Of course, you don't have to completely replace your existing IGA to leverage the power of Lumos. There is another option: augmentation.

With Lumos, IGA is about transforming identity from a risk to a strategic advantage. Ready to modernize identity governance?

Book a demo and see Lumos in action.

About Lumos

Lumos is the first autonomous identity platform. It automatically discovers and manages access across all your apps. Instead of being overwhelmed by the sprawl of apps and access, Lumos empowers organizations with one unified solution that controls access on auto-pilot.

Lumos customers can enhance security, cut software spend and boost employee productivity — all in one platform. Trusted by hundreds of companies, Lumos powers millions of access requests across global companies.

Learn more: www.lumos.com