opentext™

WHITE PAPER

Getting the most out of OpenText NetIQ Identity Governance

Processes, practices, and program guidance for scaling identity governance and administration across the enterprise.



Contents

Executive summary 4

Begin with the end in mind 5

Assemble the right team and sponsors 6

- The three characteristics every program team needs 6
- Key sponsors and stakeholders 6

A program plan that matures over time 7

- Phase 1 - Foundation 7
- Phase 2 - Improved (policy, process, and permission lifecycle) 7
- Phase 3 - Better (roles and pre-approved access) 8
- Phase 4 - Mature (self-service and orchestration) 8

The catalog: The foundation of everything else 9

- The IG data model 9
- Practices that keep the catalog healthy 9

Reviews: The heart of the program 10

- Two categories of reviews 10
- Reducing reviewer burden 10
- Certification policies 11

Fulfillment: Closing the loop 11

- Four fulfillment patterns 11
- Why fulfillment matters for scale 12
- Closed-loop verification 12

Data policies and the permission lifecycle 13

- Data policies 13
- The permission lifecycle 14

Terms, transfers, and business roles 14
Termination and transfer handling 14
Business roles: the highest-leverage capability 15
Role mining 15
Insights, reports, and metrics 16
NetIQ Governance Insights 16
Reporting 16
Metrics that resonate with leadership 17
Orchestration: Scaling to the whole enterprise 17
What to orchestrate 17
Scaling data collection 18
Measuring success and continuous improvement 18
Questions every program should answer 19
Where to get help 19
OpenText community 19
Implementation partners 19
Documentation 20
Conclusion 20

Executive summary

Acknowledgment: *Much of the practical guidance in this paper is informed by the work of Jim Montgomery, IGA practice lead with OpenText partner TriVir. Montgomery's IGA Tech Dive video series and webinar Scaling IGA to Cover the Whole Enterprise have shaped how many clients and partners approach NetIQ Identity Governance deployments.*

Most organizations that purchase an identity governance and administration (IGA) platform such as OpenText™ NetIQ™ Identity Governance are trying to solve a handful of urgent business problems: they need to pass audits, reduce risk, lower the cost of insurance, and prevent the loss of contracts that depend on a strong security posture. They buy the software, stand up the servers, onboard a few applications, and run a first review, and quickly discover that the technology alone does not produce a successful governance program. It's vital to pair the identity governance (IG) platform with the right processes and people, and a disciplined program plan that matures over time.

This paper distills practical guidance for getting the most out of NetIQ Identity Governance, drawing on real-world implementation experience and the platform's own design philosophy. It is organized around the operational reality of running an IG program: assemble the right team, plan in phases, control review scope through policy, build a permission lifecycle, automate fulfillment, leverage roles, react to employment events, measure with insights and reports, and orchestrate the steady state.

Clients who follow these practices typically see immediate, measurable returns. In one example, a publicly traded organization subject to Sarbanes-Oxley (SOX) regulations decreased access to its financial systems by roughly 15% after its first review, and continued to find the same level of inappropriate access on subsequent cycles. Another client replaced spreadsheet-driven attestations with NetIQ Identity Governance and saved approximately 2,600 hours of manual review effort per cycle—roughly a quarter of a million dollars in labor.

The sections that follow cover the business case for IGA, how to build the team and program plan, the seven operational capabilities that produce the most value, how to measure success, and where to go for help.



Begin with the end in mind

Imagine that the deployment is complete. Every in-scope application has been onboarded. Reviewers are completing certifications on schedule. Auditors are receiving artifacts that prove the process. Fulfillment is closing the loop on every decision. The CISO has metrics on a dashboard. Access is being granted and revoked dynamically as people join, move, and leave.

That is the destination. Before discussing how to get there, it helps to be explicit about the business needs that drive almost every IGA program:

- **Passing audits:** Most organizations come to IGA because of audit findings, including repeat findings. They need a defensible, repeatable process that produces evidence.
- **Improving security posture:** This is done by reducing standing privilege, eliminating orphaned accounts, and ensuring that access matches current job function.
- **Lowering insurance and risk exposure:** Cyber insurance carriers increasingly require demonstrable identity controls. Strong governance lowers premiums and supports renewal.
- **Protecting revenue and contracts:** Large customers and regulators will revoke business if controls fail. A working IGA program protects existing relationships and unlocks new ones.

These goals are not technical but belong to the business. This is the most important shift for any IGA program—the program it enables is a business program, not an IT project.

Key principle

Governance rollout is not an IT-only responsibility. It is a team effort that requires sustained collaboration between IT, security, compliance, application owners, and the business. This is a meaningful shift from traditional IT projects, and recognizing it early sets the program up for success.



Assemble the right team and sponsors

A successful IGA program is not owned by a single group. If one team owns governance for the entire organization, that team becomes a bottleneck and the program cannot scale. IG must be delivered as a service that the business consumes.

The three characteristics every program team needs

Across dozens of implementations, three traits consistently separate teams that succeed from teams that stall:

- **Talent:** Someone on the team must be able to figure out what needs to happen both technically and procedurally to meet the goal.
- **Discipline:** Someone must keep the team focused on the plan, control scope, and prevent the program from chasing every interesting feature in the product.
- **Commitment:** Someone must be willing to keep going when things get hard. Governance programs always struggle in places nobody expected. Commitment carries them through.

Key sponsors and stakeholders

Beyond the core implementation team, an effective program engages a wider stakeholder community:

- **Executive sponsor (CTO or equivalent)** who carries the mandate from the board, removes blockers, and connects the program to enterprise risk.
- **VP of Information Technology** who owns the applications under review and the audit work the program is replacing.
- **VP of IT Compliance** who owns the security standards being enforced and helps translate complex regulations into review definitions.
- **Application owners** who provide the permission metadata, identify authorized reviewers, and perform completeness and accuracy checks. They are stakeholders, not victims, so bring them along early.
- **Internal compliance and audit teams** who define what artifacts are required and what “good” looks like for the auditor.
- **Integration and orchestration teams** who provide the infrastructure to onboard applications and orchestrate the steady-state governance cycle at scale.
- **Reviewers and review owners** who are frontline business users. The program lives or dies based on their experience.

A practical guideline: avoid surprising application owners with new responsibilities. Engage them early, explain the value, train them, and treat their feedback as essential. They will perform recurring work for years to come, and their goodwill compounds.

A program plan that matures over time

The most common mistake is to think of a NetIQ Identity Governance deployment as a single project with a beginning, a middle, and an end. It is not. It is a program that matures across four progressively more capable phases. Each phase builds on the one before it. The phases are cumulative, not sequential checkboxes.

Phase 1 - Foundation

Stand up the platform, onboard a few applications, run a proof-of-concept review, and prove that the technology works end to end. Phase 1 deliverables typically include:

- Servers installed, database selected (PostgreSQL, Oracle, or SQL Server), and the NetIQ Identity Governance software configured.
- Identity collector connected to the authoritative source (HR system, NetIQ™ Identity Manager, Active Directory, etc.).
- Two to four representative applications onboarded—usually the systems with the most audit pressure.
- A first access review run end to end, including reviewer training and fulfillment of resulting changes.
- Audit findings from the prior cycle mapped to the evidence that the new program produces.

Phase 2 - Improved (policy, process, and permission lifecycle)

Phase 1 will surface the first hard truth of governance: There is more access to review than there are human hours to review it. A reviewer who can make a decision in 10 seconds and has 80 hours of focused time in a two-week window can theoretically process 28,800 items. In practice, no one sustains that. The program must be constrained to what is reviewable.

Phase 2 adds policy and process around the technology:

- A written governance policy that defines scope—for example, “review administrative privileges and non-built-in accounts on systems handling regulated data.”
- Documented processes for application onboarding, reviewer assignment, escalation, and exception handling.
- A formal permission lifecycle (covered in detail in Section 5) that ensures every permission has an owner, a description, and a refresh cadence.
- Closed-loop verification reporting so auditors can prove changes were actually applied.
- A pipeline of applications to onboard next, ranked by audit risk and business criticality.



Phase 3 - Better (roles and pre-approved access)

Once the catalog has clean metadata, roles become possible. Roles are the single biggest lever for reducing reviewer burden and accelerating provisioning. Phase 3 introduces:

- Role mining to discover candidates' technical roles already present in the data.
- Business roles that grant access automatically based on identity attributes (department, title, location, employee type).
- Reviews focused on exceptions—access not covered by a role—rather than every individual permission.
- Pre-approved access requests for items authorized by a business role.

Phase 4 - Mature (self-service and orchestration)

The final maturity stage is where IG becomes a service the business consumes without IT mediation. Phase 4 adds:

- Application owner self-onboarding, so the IT team is not a bottleneck for adding the fiftieth, one hundredth, or five hundredth application.
- Training programs for reviewers, review owners, and application owners, ideally delivered through the enterprise training tool.
- Orchestration through ServiceNow, Remedy, or a similar tool to automate completeness and accuracy checks, kick off collections, schedule reviews, and chase down stale tasks.
- API-driven automation, making every action available in the IG interface available through the REST API, which means the entire governance cycle can be scripted.

Who does the work as the program matures?

IT implementation team responsibilities: Installing software, mapping data into the standard model, maintaining the platform, and supporting collectors and fulfillers.

Business responsibilities: Defining policy, identifying reviewers, describing permissions, training users, certifying access, and confirming completeness and accuracy of source data.

The IT share of steady-state work shrinks as the program matures. By Phase 4, the business consumes governance as a service, and IT does very little of the recurring work.

The catalog: The foundation of everything else

Every NetIQ Identity Governance capability depends on the catalog, including reviews, requests, fulfillment, roles, insights, reports, and policies. The catalog is a single pane of glass that presents access information from every connected system in a common format. Get this right and everything else becomes possible. Get it wrong and the program never gets off the ground.

The IG data model

NetIQ Identity Governance represents the world with a small set of object types:

- **Identities:** One logical record per human, sometimes called a "belly button account." Every account in every application links back to one identity.
- **Accounts:** An account in a specific application (an Active Directory user, an Oracle EBS account, a SaaS login).
- **Permissions:** Anything granting access: group memberships, roles in the source system, entitlements, file shares. A type attribute differentiates a group from a role from any other kind of grant.
- **Applications:** The containers that hold accounts and permissions and the metadata about how the data was collected.

Because everything is normalized into this model, a reviewer sees the same review interface and the same decision flow whether they are reviewing Active Directory, SAP, Salesforce, or a custom mainframe application. This consistency is critical to scale—training a reviewer once is enough.

Practices that keep the catalog healthy

- **Map every application into the standard data model**
  The application attributes on the right side of the collector configuration must be carefully mapped to the IG attribute names on the left. Inconsistent mapping is the root cause of most catalog issues.
- **Collect the attributes that meet fulfillment needs**
  Some fulfillers require specific attributes (distinguished names, account identifiers, group references) to make changes back to the source. Plan for these during collector setup, not after the first failed fulfillment.
- **Set ownership at collection time**
  Every account needs a holder (the person who uses the access) and a custodian (the person responsible for the account). Every permission needs an owner. Missing owners are the single most common cause of reviews that cannot be assigned.
- **Refresh on a schedule that matches your risk tolerance**
  Time-based reviews are only as accurate as the data behind them. If access can change daily, weekly collection is not enough.

Reviews: The heart of the program

Performing reviews of access is the primary function of NetIQ Identity Governance. A review definition specifies what is being reviewed, who is reviewing it, and the criteria for completion. When a review owner starts a run, tasks are distributed to reviewers, who decide to keep, modify, or remove each item. Review owners approve completed work, and fulfillment kicks off changes back to the source systems.

Two categories of reviews

Every governance program needs both types operating in parallel:

- **Time-based reviews:** Periodic certifications done quarterly, semiannually, or annually. These are the catch-alls that confirm ongoing access is still appropriate and cleans up anything missed by other processes.
- **Event-based reviews:** Triggered by something that happened—a termination, a department transfer, a title change, a risk-score spike, a missing attribute—these are typically small in scope (one user, one application) but high in urgency. Event-based reviews are how the program reacts in near real-time instead of waiting months for the next cycle.



Reducing reviewer burden

Reviewer fatigue is the single greatest threat to a governance program. Reviewers become overwhelmed by rubber-stamp decisions, which destroys the program's credibility with auditors. Five practices protect reviewer time:

- **Scope reviews narrowly:** Review only what policy requires, typically administrative privileges and access to systems handling regulated data, not every group membership in the directory.
- **Use roles to consolidate:** Reviewing a single role assignment is much faster than reviewing the ten permissions inside it. Reviewers can certify the role and only drill into exceptions.
- **Use multi-stage reviews:** Route routine items to first-line reviewers and escalate only flagged items to senior staff.
- **Provide context:** Every review item should include permission descriptions, last-used data where available, risk scores, and the reviewer's relationship to the user.
- **Use micro certifications:** A micro certification is a focused, event-driven review covering a small set of items, typically the result of a policy violation. Micro certifications eliminate the need for full-scale reviews in many situations.

Certification policies

Certification policies bundle related review definitions into a single compliance view. For SOX compliance, for example, an organization can create a certification policy that includes every review covering systems that process SOX-relevant data. The policy reports violations, tracks status, and produces consolidated audit artifacts. This is what auditors want to see, not a stack of individual review reports, but a single certification status against a named control.

Fulfillment: Closing the loop

A review decision is worthless if the change does not actually happen. Fulfillment is what makes NetIQ Identity Governance more than a sophisticated spreadsheet. Every decision—from a review, from a request, from a business role detection, from a data policy remediation—produces a fulfillment item. The fulfillment system tracks each item to completion and verifies the change on the next collection cycle.

Four fulfillment patterns

NetIQ Identity Governance supports four patterns for getting changes back into the source systems. Most enterprises use a combination, chosen per application based on what is available and what scales:

Pattern	When to use
Ticketing system	ServiceNow, Remedy, or a similar ticketing tool is usually the first phase for any application. Fulfillment creates tickets that humans process; it's the slowest but easiest to set up.
Direct fulfillment	NetIQ Identity Governance talks directly to the target system (Active Directory via LDAP, for example) and makes the change. This is fast, fully automated, and out of the box for many systems.
NetIQ Identity Manager	If an IDM driver already manages a system, NetIQ Identity Governance hands changes to NetIQ Identity Manager via entitlements, roles, or resources. The existing driver does the work. This is the simplest path when NetIQ Identity Manager is already deployed.
Integration platform	An enterprise service bus or integration tool maintains connections to many applications. NetIQ Identity Governance hands fulfillment to the integration platform. This is best for large estates with hundreds of applications.

Why fulfillment matters for scale

The flexibility of NetIQ Identity Governance fulfillment is one of the primary reasons the platform scales to thousands of applications. The IG team does not have to own credentials and connection information for every target system. That responsibility can be offloaded to an integration team or platform. Fulfillment is configured per application with change types for adding or removing accounts, permissions, and roles. All of it uses the same underlying engine.

Why this matters

A robust fulfillment system is what makes NetIQ Identity Governance more than a sophisticated spreadsheet. The ability to actually carry out the decisions made during reviews and verify those changes on the next collection is what produces the audit artifacts and security improvements that justify the program.

Closed-loop verification

Fulfillment items remain open until a subsequent collection verifies that the change actually happened in the source system. This closed-loop verification is what auditors are looking for. It is not enough to show that a reviewer made a decision; the artifact has to show that the decision was carried out. NetIQ Identity Governance's verification report is one of the highest-value audit artifacts the program produces.



Data policies and the permission lifecycle

Two complementary practices keep an IGA program healthy between review cycles: data policies that catch problems automatically, and a permission lifecycle that keeps the catalog reviewable in the first place.

Data policies

Data policies interrogate the catalog and react when something is missing, changed, or wrong. They come in two flavors:

- **Collection data policies:** Evaluate what is being added, removed, or counted during data collection. Useful for detecting bulk changes—a 10% spike in accounts collected from a system, for example.
- **Publication data policies:** Evaluate the published catalog, including changes to attributes such as title, department, or supervisor.

Each policy can take one of four remediation actions when it fires:

- Send an email notification to the appropriate owner, supervisor, or administrator.
- Create a change request that flows into fulfillment.
- Start a workflow for a richer response.
- Kick off a micro certification scoped to the specific item detected.

A few high-value data policies that almost every program should implement:

- **Accounts without owners:** Kick off a micro certification asking the application owner to designate one.
- **Identities without supervisors or email addresses:** These attributes are essential for governance, since missing values block reviews.
- **Permissions without owners or descriptions:** Permissions that cannot be described to a reviewer cannot be reviewed.
- **Risk-score spike:** When a user's risk crosses a threshold (for example 90%) a focused review is triggered by their supervisor.
- **Bulk changes:** Alert when the volume of changes on a collection exceeds a threshold, which is a possible sign of a misconfigured source or compromise.

The permission lifecycle

Permissions have a lifecycle just like users do. New permissions are introduced when applications are added. They are granted and revoked over time. Their descriptions need to stay accurate. Eventually, when the application retires, the permissions are removed. Application owners, not the IG team, are responsible for maintaining permission metadata. They know what access does and who should have it.

A working permission lifecycle includes three application-owner responsibilities:

- **Completeness and accuracy:** Before each review cycle, the application owner confirms the collected data is correct and complete.
- **Authorized reviewers:** The application owner identifies who is allowed to review what, including escalation paths.
- **Permission updates:** Names, descriptions, owners, and risk classifications are kept current. A permission with a stale description from five years ago cannot be reviewed honestly.

Terms, transfers, and business roles

Two capabilities convert governance from a periodic activity into a continuous control: Event-based handling of terminations and transfers and business roles that automate provisioning and deprovisioning.

Termination and transfer handling

When an employee is terminated, their access should be removed quickly—ideally before they leave the building. When an employee transfers to a new role, access that was appropriate for their old job is usually no longer appropriate for their new one. NetIQ Identity Governance handles both cases the same way: A publication data policy watches for the change and when it fires a micro certification is launched (or in mature programs, access is revoked or adjusted automatically).

A typical termination flow:

- The NetIQ Identity Manager driver (or another identity collector) picks up the employee-status change from HR.
- On the next IG polling cycle, the new status arrives in the catalog.
- A publication data policy detects the change to “terminated” and fires its remediation.
- The remediation runs a micro certification on the user’s full access, routed to the supervisor.
- The supervisor decides whether to revoke each item or transfer it to a successor, and fulfillment carries out the decisions.

The transfer flow is similar, triggered by a change to title or department. Because the scope is one user, the review completes quickly—usually within days, not the months a time-based review would take.

Business roles: the highest-leverage capability

Business roles may be the single most impactful capability in NetIQ Identity Governance. A business role does two things at once. It defines membership criteria based on identity attributes ("users whose department is Finance"), and it defines mandatory and optional access for members. When a user joins the role, missing mandatory access is fulfilled automatically. When a user falls out of the role, perhaps because of a department change, they lose access, optionally after a grace period.

The implications are profound:

- **Onboarding becomes automatic:** A new hire whose attributes match a business role receives their required access the moment HR data arrives, with no help desk ticket.
- **Department transfers self-correct:** Access that depends on the old department is revoked automatically; access for the new department is granted.
- **Reviews shrink dramatically:** Business-role-authorized access can be excluded from reviews or reviewed only at the role level. Reviewers focus on exceptions, not the steady state.
- **Requests become pre-approved:** Optional access associated with a role is approved instantly when requested because the role already authorized it.



Role mining

Identifying the right business roles is hard. Role mining uses machine-learning analytics over the access NetIQ Identity Governance has already collected to suggest candidate roles. The tool can work top-down (start from an attribute such as department or title and find common permissions) or bottom-up (start from sets of permissions and find the user populations that share them). The output is a set of role candidates with thresholds the administrator can tune (for example, "include permissions held by at least 75% of members"). Promote the good candidates to draft business roles, refine them with the business, and publish.

Insights, reports, and metrics

A governance program lives or dies by what it can show leadership. NetIQ Identity Governance provides three complementary capabilities for producing the data, evidence, and metrics that leadership needs.

NetIQ Governance Insights

NetIQ™ Governance Insights is a lightweight business-intelligence tool inside NetIQ Identity Governance. It lets administrators build queries directly against the catalog without exporting to a separate system. Common uses include:

- Finding all permissions across all applications with a specific attribute value (for example, every entitlement tagged with a particular department).
- Finding accounts in a system that are missing custodians.
- Listing review items approved by a specific person within a date range.
- Building cross-references between objects—for example, joining review items with the users who approved them.

Insights queries can be saved, scheduled, and emailed to stakeholders as CSV attachments. They are the right tool for ad-hoc questions and ongoing intelligence.

Reporting

The reporting system produces formal PDF and CSV artifacts. Reports are the system of records for audits. Key reports every program should run:

- **Review coverage overview:** Identifies accounts, permissions, roles, and users that are not included in any review—a critical gap analysis.
- **Reviewer status and reviewer overview:** Show whether reviewers are completing their work on schedule.
- **Reconciliation:** Compares the desired state (per NetIQ Identity Manager or another source of truth) with the current state in each connected system.
- **Unauthorized permissions by user:** Lists permissions not authorized by any business role—the prime exception population.
- **Privileged account ownership:** Maps privileged accounts to the users who own them, grouped by application.
- **Reviews with deleted stakeholders:** Highlights review definitions that reference owners, reviewers, or auditors who no longer exist—a common quiet failure mode.

Metrics that resonate with leadership

NetIQ Identity Governance tracks activities and key risk indicators that administrators can use to build dashboards. Defaults include average users per account, count of unmapped accounts, and the proportion of entitlements assigned by policy versus directly. Custom metrics can be defined using SQL or insight queries. The metrics that consistently resonate with executives include:

- Percentage of access removed per review cycle (a benchmark of 15% is not unusual on the first cycle in many environments).
- Time-to-revoke after a termination—how quickly access actually disappears.
- Percentage of access granted through roles versus exception.
- Number of applications under governance and percentage of in-scope applications covered.
- Hours saved per review cycle versus the prior manual process.
- Number of audit findings closed and prevented.

Orchestration: Scaling to the whole enterprise

By the time a program reaches Phase 4, the steady-state governance cycle has many steps: Collect data, run completeness and accuracy checks, allow application owners to confirm or correct, refresh data, kick off the review, monitor progress, complete the review, fulfill changes, verify changes, produce reports. Doing this manually for 50 applications is painful. For 500, it is impossible.

This is where orchestration comes in. Every action available in the NetIQ Identity Governance user interface is also available via the REST API. Anything that can be clicked can be scripted. That makes the platform an ideal partner for an enterprise workflow tool such as ServiceNow, Remedy, or a custom orchestration platform.

What to orchestrate

- **Application onboarding:** Provide a self-service onboarding flow for application owners. They register the application, the orchestration tool drives collection, mapping validation, and initial review creation, with the IG team only stepping in for exceptions.
- **Completeness and accuracy checks:** After each collection, automatically present application owners with a confirmation task. Their sign-off triggers the review.
- **Permission-lifecycle updates:** When an application changes, route updates to the right owner via the workflow tool rather than asking them to log into NetIQ Identity Governance.
- **Review scheduling and chasing:** Use the orchestration tool to start reviews on schedule, monitor completion, escalate stragglers, and notify owners when reviews close.
- **Reporting and distribution:** Generate reports on a schedule and deliver them through the enterprise distribution channels stakeholders already use.

Scaling data collection

As application count grows, the IG team should not be the bottleneck for connection credentials and host information for every system. An integration platform—an enterprise service bus, a SCIM provider, or an existing IDM deployment—can own those connections, transform the data, and present it to IG for consumption. On the fulfillment side, the same integration platform can apply the changes back. This pattern dramatically reduces the IG team's operational load and aligns identity governance with the organization's broader integration strategy.

API-first automation

Everything that is possible in the NetIQ Identity Governance user interface is also available through the REST API. With an orchestration tool, the entire governance cycle—kicking off reviews, generating reports, collecting data, publishing data, fulfilling changes—can be automated. This is the foundation that allows the platform to scale to hundreds or thousands of applications without proportional growth in IT effort.

Measuring success and continuous improvement

A mature NetIQ Identity Governance program produces evidence on demand: Audit artifacts ready to share without manual assembly, clear policy and process documentation, closed-loop verification reporting that proves changes were carried out, reduced reviewer burden, demonstrable reductions in standing privilege, and the passing audits and retained contracts that follow. Customer experience consistently shows fast, measurable returns. One publicly traded organization connected NetIQ Identity Governance to its Oracle E-Business Suite financials and reduced access by 15% in the first review and continued to reduce roughly 15% on each subsequent cycle, evidence of constant access churn that no manual process could catch. A separate large-enterprise client saved approximately 2,600 person-hours per review cycle—roughly $250,000 per cycle in labor—by replacing manual collection and spreadsheet attestation. In both cases the deployment paid for itself many times over within the first year.



Questions every program should answer

Every program team should be able to answer these questions clearly:

- Who owns the security standard being followed, and is there a team responsible for process and policy?
- Who are the right reviewers, and do they have enough information to make good decisions?
- How often are reviews performed, and what is the artifact that satisfies the auditor?
- Are we going wide (many applications, fewer features) or going deep (every feature, fewer applications)? Both are valid; the choice should be deliberate.
- Which application is being onboarded next, and what is the criteria for choosing it?
- What metrics are being shared with leadership, and how are they trending?

Where to get help

No governance program runs perfectly the first time. The good news is that NetIQ Identity Governance has an active client and partner community ready to help.

OpenText community

The OpenText Identity Governance community is where clients, partners, and OpenText engineers exchange questions, ideas, and tips. Active areas include:

- Community home
- Discussions
- Ideas exchange
- Tips and news
- Cybersecurity blog

Implementation partners

OpenText maintains a network of implementation partners who provide advisory and implementation services in the identity and access management realm. These partners have completed many of these deployments; they know where the hard parts are, and they can take on the initial heavy lift while the team builds internal capability. Engaging a partner early—especially Phases 1 and 2 — is often the difference between a program that lands and a program that stalls.

Resources

OpenText NetIQ Identity Governance | IGA Solutions ›

What is Identity Governance and Administration? ›

Documentation

Definitive product documentation is available in the OpenText Identity Governance User and Administration Guide, the Workflow Administration Guide, the Form Builder Guide, the Reporting Guide, and the Collectors and Fulfillers Configuration Guide, all maintained at the OpenText documentation site for the current product version.

Conclusion

NetIQ Identity Governance is a powerful platform. The clients who get the most out of it treat it as the engine of a business program, not a piece of software the IT team operates. They assemble a team with talent, discipline, and commitment. They engage business stakeholders early. They mature their program in deliberate phases. They invest in a healthy catalog, scope reviews carefully, automate fulfillment, build out roles, react to employment events, and orchestrate the steady state. They measure what matters and report it to leadership. The result is a deployment that covers the whole enterprise, produces audit-ready artifacts on demand, demonstrably reduces risk, and frees the business to focus on its real work—and clients who follow the practices in this paper consistently get there.

Copyright © 2026 Open Text • 06.26 | 262-000227-001

opentext™