Whitepaper

Identity governance buyer's guide

Contents

Why is Identity governance important now

There is an explosion of digital identities in the workplace, fueled by people, devices, and resources spread across the globe. Cloud and SaaS adoption, remote and contract workers, and mobile devices have increased Identity management complexity. It's difficult for IT and security teams to balance workforce productivity with the need to limit access to only the right people, the right resources, and for the right amount of time. Inadequate management of identities can lead to security gaps across the Identity lifecycle, which can leave organizations vulnerable to breaches. Similarly, managing an interconnected ecosystem of users, resources, and Identity stores can result in manual processes and workloads that grow as an organization's workforce and technology footprint expands. As a result, 61% of businesses now see managing and securing digital identities as a top three priority of their security program[1].

The purpose of Identity governance and administration (IGA) is to manage the complex array of an organization's access rights across its various resources and identity repositories. IGA combines

- Identity governance: processes and policies that cover role management, access reviews or certifications, separation of duties, logging, analytics, and reporting
- Identity administration: administering accounts and credentials; provisioning and deprovisioning users, service accounts, and devices; and managing entitlements

Identity Governance and Administration (IGA) answers the following questions:

- Who has access to what?
- When did they get access?
- How did they get access?
- Should they continue to have access?
- Does the access create a compliance conflict?

[1] 2023 Trends in securing digital identities, Identity Defined Security Alliance

Benefits of implementing IGA

While most organizations think IGA solutions largely focus on the world of compliance and Identity control requirements, they have other benefits.

- **Better security outcomes with least privilege access**. Organizations are implementing least privilege access to resources as part of their Zero Trust strategy, ensuring users are given only the minimum levels of permissions needed to do their jobs. IGA capabilities can inform risk-based cybersecurity programs by implementing fine-grained, least privilege access controls consistently throughout an organization's users and resources.
- **Improved operational efficiency**. When implemented correctly, IGA can automate common tasks for users and IT teams, increasing productivity and satisfaction. For example, automated access requests can streamline the process of granting new permissions to users. Leveraging automation for provisioning and deprovisioning can reduce manual data entry tasks and the risk of associated errors.
- **SaaS visibility and software rationalization**. Implementing least privilege access to apps and entitlements can also reduce over-provisioning and the costs associated with extra software licenses and their maintenance. IGA capabilities can discover and remediate over-provisioned applications.

Technology challenges with implementing IGA

While a majority of organizations see investing in IGA solutions as a priority, there are some significant barriers to adoption.

- **Fragmented identity stores.** Organizations often have different identity repositories for different cloud, on-prem, and hybrid environments, creating Identity silos rather than single sources of truth. Similarly, many organizations use HR systems for full-time employees but may use a different system to manage contractors and other non-employees. When security and Identity professionals were asked what barriers prevent their company from doing more to secure identities, the top reason cited was:

> "Identity frameworks are complicated with multiple vendors and different architectures[2]."

- **Diverse technology ecosystem.** Complex technology environments are a barrier to adoption, as many different resources must connect to or integrate with IGA systems. Every connector or integration created by an organization requires specialized skills to develop, test, and maintain. With public cloud and SaaS adoption growing by 21% and 18% a year, respectively[3], ensuring users have the right access and permissions for a wide range of resources, each with their own roles or permissions, is becoming very complicated. This can lead to over-provisioning that puts the business at risk. One report suggests that more than 95% of accounts in IaaS use less than 3% of the entitlements they are granted[4].
- **Complex technology ownership.** Lines of business or departments may have their own software tools that fall under an organization's compliance policies. This puts IT and Governance, risk, and compliance (GRC) teams in the difficult position of enabling least privilege and overseeing compliance audits on resources they do not administer. This lack of visibility and control can lead to gaps in security and compliance.

With this in mind, let's look at some of the considerations for choosing an IGA solution.

[2] 2023 Trends in securing digital identities, Identity Defined Security Alliance

[3] Gartner Forecast: Public Cloud Services Worldwide, 2021-2027, 1Q23

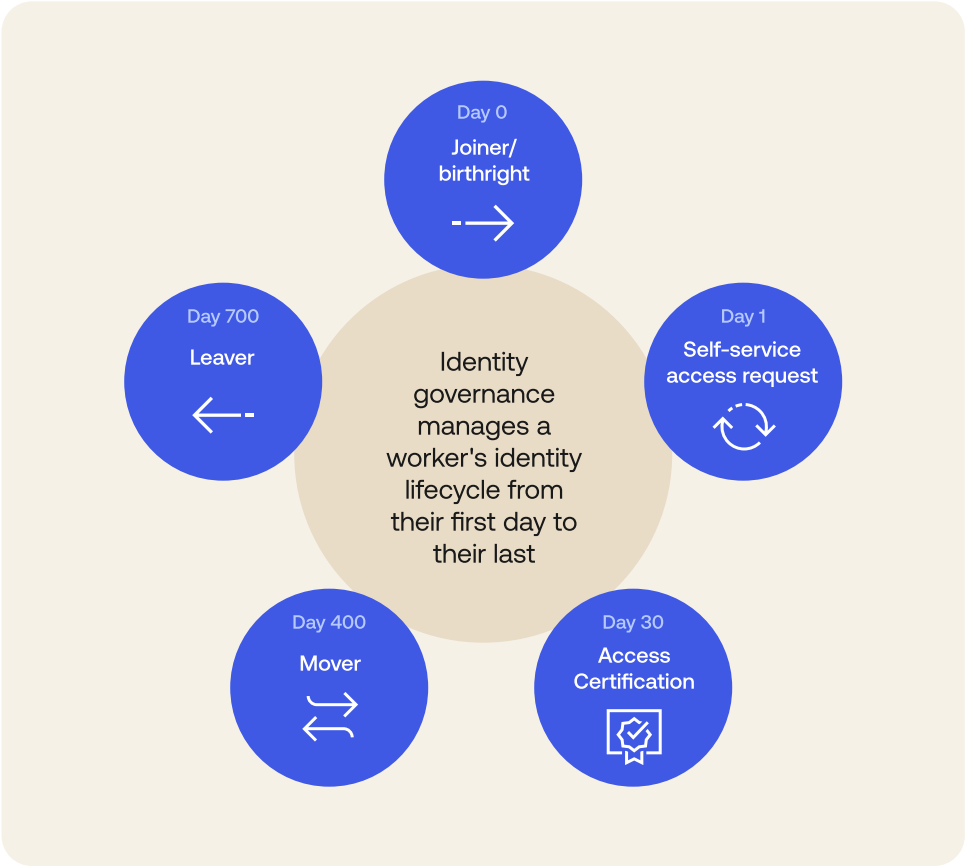
[4] Innovation Insight for Cloud Infrastructure Entitlement Management, Gartner

IGA use cases

Before choosing an IGA solution, the first step is to define what it needs to do for your organization. While there are many uses for Identity Governance, most organizations prioritize these most common use cases.

- **Identity lifecycle management:** Manage the joiner, mover, and leaver processes of an organization across cloud and on-prem resources, including application access requests and finer-grained, entitlements-based access controls within an application.
- **Least privilege access:** Support a Zero Trust strategy and better manage Identity risk by creating processes that limit access to only that which is required for a specific role or project.
- **Compliance:** Establish processes to document access requests, justifications, approvals, reporting, and recurring access certifications to meet compliance thresholds for a range of regulatory frameworks.

While an organization may have several use cases for an IGA solution, when it comes to implementation, it's a best practice to choose one to start.



IGA capabilities

Depending on your use cases and goals, you may not need every capability in an IGA solution. The table below gives an overview of each capability and some features and factors to consider when choosing the capabilities you need.

Capability	Detail	Considerations
User and application provisioning/ deprovisioning (also known as Identity lifecycle management)	Integrate with HR and other systems to create new user accounts, provision the apps the users need based on attributes, and schedule the identity and accounts to go live on each user's start date. Similarly, schedule deprovisioning based on data from HR or other systems for a user's retirement, job or role change, or contract termination. Automating these tasks ensures that workers can hit the ground running on their first day without significant manual effort.	• Number and types of data sources you need to integrate with (HR systems, LDAPs, Google directory, downstream applications, CSV files) • Ability to quickly deprovision across all apps on demand, i.e., in case of termination • Ease of integration to downstream applications and resources
Access requests	Streamline and codify the process for users to request access to new apps, and for approvers to review and approve/reject requests. Least privilege access often means users need to request access based on the role or project changes.	• Flexibility in access review flow and approvals • Ability to create time-bound request flows • How easily users can initiate self-service requests • How users/approvers are notified about the progress of requests • Ability to surface user context to reviewers
Access reviews/ certifications	Regularly review user access to resources to pass audits, reduce risk of inappropriate access and avoid accumulated privilege, and identify inactive accounts.	Ability to • Run campaigns by user, group, or resource • Schedule access campaigns • Run campaigns on demand • Trigger certifications automatically based on events, such as a user changing roles or departments

Capability	Detail	Considerations
Workflow orchestration	Automate and orchestrate workflows that operate across your technology environments, optimizing operations and driving efficiencies throughout compliance and risk-based Identity governance processes.	• Ability for administrators to create workflows, i.e., no-code or low-code, vs. developers • Ability for administrators to create complex workflows i.e., loops or branches • How processes and outcomes are recorded for audits/compliance • Ability for administrators to create custom workflows
Reporting and analytics	Track and present Identity governance data. Gather and analyze data to reduce access risks, streamline access requests, or other goals.	• Available out of the box reports • How easy it is to build your own reports • Visibility across ecosystem for reporting and risk signals • Ability to run reports on demand to provide evidence for audit.
Entitlement management (often called fine-grained entitlements)	Discover, provision, update, and revoke entitlements (permissions that allow users to perform specific actions in an application).	Ability to • Discover and manage on-prem and cloud apps • Detect dormant entitlements • Identify regulated entitlements
Separation of duties (or Segregation of duties or SoD)	Define and manage controls to ensure that no one person acting alone can complete a sensitive task. Minimize the occurrence of fraud, sabotage, theft, policy violations, misuse of information, and other security incidents that lead to data breaches by preventing overlaid IT access that would allow compromising activities	• Ability to limit toxic combinations via configuration • Right-size approach based on number of applicable apps and combinations

Implementation best practices

Mitigation strategies

IGA solutions have lots of capabilities that can fulfill many uses. However, as with any project, the best way to make measurable progress is to pick one use case and see it through to completion. To ensure success, any IGA implementation should have business-level, and ideally executive-level, agreement on what use case will be implemented first and which elements will be incorporated into the project. This depends on organizational priorities and pain points. For example, an organization with large, far-flung field teams may decide that automating and governing access requests and entitlements for their CRM app is the highest priority. An organization with regular staff turnover and long wait times for IT support may prioritize automating the joiner and leaver processes. Another organization spending lots of money and effort on demonstrating compliance with mandated financial regulations may prioritize governing access and entitlements for applications related to that regulation. As part of defining the project, information you will need includes

- A software asset inventory that defines the technical and business owners
- The data source(s) for Identity
- The applications that you will prioritize for the project

Whether your first use case is a pilot or a full-fledged project, you may want to limit the number of applications and entitlements. Based on our experiences and those of our customers, consider starting with a small set of applications with coarse-grained access, and if using entitlements, start with one application. This will allow you to apply lessons learned to subsequent IGA phases.

Establish compliant-by-design Identity management processes

Before implementing any technology, stakeholders should work together to define Identity management policies for resources, codifying who has access to what, when, and for how long. For IGA deployments, typical technology stakeholders include IT, GRC, and security teams. In contrast, business stakeholders are often HR teams and other departments that either own data source systems or will interact with the IGA solution in a significant way. Establishing processes that meet the highest regulatory compliance thresholds for resources within scope eliminates much of the burden associated with quarterly or annual audits.

While these processes depend on the use case(s) you are prioritizing, some examples include

- Defining approaches to attribute-based or role-based access controls for birthright access
- Defining joiner, mover, and leaver lifecycle processes
- Determining the right authentication policies for sensitive applications and data
- Codifying a process for provisioning ad hoc access via access requests
- Establishing recurring and automated access certifications, including identifying the right approvers for the users and apps and resources they connect to
- Determining when to trigger ad-hoc user reviews, such as when a user role or department changes
- Identifying toxic combinations throughout business processes and implementing guardrails to prevent infractions and pass audits

This exercise is a good time to simplify and standardize request workflows. Gartner, in their "Critical Capabilities for Identity Governance and Administration" (June 2018) report, stresses that IGA projects should focus on business process re-engineering and try to adopt a standard (linear) approval workflow across all requests rather than adopting a unique one for each application. They even recommend a simple four-stage pattern: Policy Analysis, Manager Approval, Resource Approval, and Control Approval. Of course, this may not be possible for all your business processes, which may require branching, loops, or other actions. However, defining these processes before an IGA deployment may help narrow your product selection and project scope.

This exercise also has the advantage of defining which applications and resources IGA systems need to connect to and the depth of integration required.

Establish a single source of truth

An organization's ability to effectively govern its users' access is predicated on integrating with the identity stores that organization relies on, as well as the downstream resources that organization wants to govern.

Organizations must identify their various Identity stores and work to integrate them deeply with their IGA solution, enabling attribute mapping and syncing to maintain a tight-knit reflection of the various sources. IGA systems that have flexible sourcing models that can fit a broad range of directories and integrate with multiple sources, whether they be HR information systems (HRIS), LDAPs, downstream applications, or even CSV files.

IGA systems must also be able to apply attributes or roles to downstream resources through provisioning and deprovisioning actions. Look for both coarse-grained and fine-grained entitlement integrations across a broad set of applications to suit cloud and on-prem use cases, emphasizing easily configurable integrations versus those requiring extensive professional services to implement.

Automate Identity processes

Automated processes are operationally efficient, improve end-user experiences, and reduce misconfiguration errors that can open an organization up to risk. Start with provisioning and building attribute- or role-based access controls that rely on HR system-sourced identities. As an individual joins or moves within an organization, HR updates should automatically push to new attributes or roles, updating group membership and resource access and documenting the changes for audit purposes.

Automation can also play a big role in access requests and access certification processes by eliminating the need for manual work and establishing consistent data collection — such as justifications and manager approval timing or time-bound access — for GRC teams to provide to auditors.

The deeper and broader automation is within a GRC team's designs, the less frequently an auditor will need to test processes. Once an IT or GRC team can demonstrate a working automated design, auditors only have to look for changes to the given design rather than relying on individual access control measures to look for compliance issues.

Beyond recurring flows, ensure you can build automated processes that can be triggered by certain events. For example, if a high risk login event occurs for a critical resource, that event could trigger an automated access review of that user's access capabilities.

Empower decision makers

Making informed, timely access decisions involves connecting the right people to the right processes at the right time. Building the right stakeholders into governance workflows eliminates the work of chasing down managers and application owners and creates a paper trail you can use to demonstrate compliance. Consider how you will

- **Configure workflows** that will select the right reviewers, in the right order, for access requests or certification campaigns. A best practice for access requests is to first have the user's manager review it, followed by the policy owner of the resource/application, followed by a review by information security staff.
- **Create a consistent, simple experience** for reviewers that gives them the contextual information they need to make a decision, ideally from a single screen. For example, present important information such as: the requester's title, department, and justification for why they are initiating the request; the manager's comments on the need to access a certain project; and the security team's comments on appropriate access duration.
- **Establish automated processes** that disseminate access governance requests and decisions, keeping teams informed and productive. For example, if a user has their access revoked, the user and their manager should be informed should they want to reinstate access. Similarly, if a user requests access, ensure all stakeholders can easily see the progress of the request and maintain productivity with reminders that reviewers can easily follow up on.

Attributes to evaluate in an IGA solution

Regardless of your use cases, these key attributes can contribute to a faster, more efficient, and more successful deployment.

Unified Identity platform

As organizations deprecate on-premises systems and move workloads to the cloud, the overlap is increasing between the problems Identity and Access Management (IAM), privileged access management (PAM), and IGA systems solve. By 2025, 70% of new access management, governance, administration, and privileged access deployments will be converged IAM platforms[5].

There are many operational advantages to a unified platform. A single view of all organizational identities offers

- **Ability to reduce Identity risks**. The comprehensive view that a unified platform provides can offer valuable insights that help you detect and respond to Identity threats. For example, IAM can deliver risk signals that inform governance and privileged access decisions while triggering reviews. An elevated risk profile based on a user's behavior when logging in could trigger a certification campaign, reduction in user privileges, or even suspend access to a resource.
- **Faster time to value**. A single pane of glass to manage identities, access, and governance shortens the implementation time for organizations and reduces the cost of maintaining multiple systems.
- **Improved user experiences**. Providing end users and administrators with single interfaces for requests, processes, and decisions reduces the potential for mistakes and increases the productivity of everyone in the organization.

Integration support

At a minimum, Identity governance solutions need to exchange information with many different Identity sources, including HR information systems (HRIS) or other systems of record, data stores, and IAM systems. When you add automation, IGA systems may integrate with many more apps in your technology stack. For example, integrations with IT service management (ITSM) systems can simplify the process for users initiating access requests, while integrations with collaboration tools can simplify the approval process for people reviewing access requests.

---

[5] Gartner Research

Building each integration can take weeks or months, and each comes with ongoing maintenance and support costs. As the number of integrations mount, so does the complexity of creating and maintaining connectors to apps and data stores. Support for integrations is the number one concern we hear from customers who are thinking about implementing an IGA solution. The greater the requirement for development and customization, the slower the implementation time.

An IGA solution with out-of-the-box, configurable integrations to needed apps and resources reduces the organizational burden associated with building, testing, and maintaining a custom integration.

Usability

While IGA outcomes stress security and compliance, it should not come at the expense of usability. Implementing IGA impacts all users in an organization since it changes how users request and receive access to applications and systems. Making it easy for end users to request access to applications or change permissions will reduce training requirements, increase access request adoption, and positively impact productivity.

Options for improving end-user experiences include

- Connecting the IGA system with familiar and collaboration tools to enable end users to manage access requests from familiar interfaces
- Creating self-service experiences where end users can track access requests and monitor approvals themselves via real-time workstreams

Also consider usability for workers administering the IGA solution. Ways to make administrators more effective include

- Utilizing no-code tooling to build out workflows rather than relying on scripting
- Minimizing the number of consoles and tasks required to launch access certifications and build reports
- Enabling bulk actions, such as access requests or entitlements for a project group
- Ability to filter and download reports by users and resources

Usability for GRC teams is another consideration. For example, it may be an advantage for GRC teams to run access certification campaigns themselves without relying on administrators.

How Okta can help

Workforce Identity Cloud is a cloud-native, converged IAM, IGA, and PAM platform that provides an unparalleled view of user identity.

Okta Identity Governance is a SaaS-delivered solution within the Workforce Identity Cloud that simplifies and manages your Identity and access lifecycles across multiple systems and improves your organization's security posture. With Okta's more than 7,000 pre-built integrations, including more than 600 directly related to Identity Governance, you can deploy quickly and automate complex Identity processes at scale.

Okta Identity Governance enables organizations to:

- Efficiently create, protect, and audit access to critical resources.
- Improve security by
    - Reducing risks associated with unmanaged identities and accumulating elevated or privileged access.
    - Making access certification more meaningful with insight from the converged IAM solution, such as sign-in frequency, a resource's last accessed date, and more.
    - Giving appropriate access and entitlements to sensitive data and apps with automated workflows that enable appropriate reviewers to evaluate and approve who receives access.
    - Triggering user certification when detecting suspicious user activity or when a user changes roles.
- Increase employee productivity by
    - Automatically provisioning new employees to birthright apps based on their user profile attributes, enabling them to be productive from day one.
    - Enabling convenient self-service access requests to any Okta resource from their workplace collaboration tools.

- Contain costs by discovering orphaned or over-provisioned account access to applications.
- Improve operational efficiency by
    - Automating tasks to reduce the time taken and errors associated with manual data entry and provisioning tasks.
    - Deploying a governance solution more quickly and easily than alternatives with out-of-the-box integrations to popular apps.

For an overview of Okta Identity Governance, read the solution brief or watch this short video. For more information on meeting compliance obligations with Okta Identity Governance, download the white paper.