Guide

The 6 most common pitfalls of Identity Governance and how to avoid them

Omada

Do more with identity

Table of Contents

Introduction

Identity governance and administration (IGA) is an important tool that helps organizations ensure that the right people have the right access to the right resources for the right reasons at the right time.

When deployed properly, IGA helps ensure that everyone has access to the applications and data they need to perform their jobs, and security and audit teams have all the proof on the back end that access is up-to-date, and no excessive privileges or entitlements are granted.

IGA consists of a set of core competencies:

- **Connectivity and fulfillment.** Synchronize identity attributes and access entitlements from authoritative sources, as well as provision and deprovision access to connected systems
- **Identity lifecycle management.** As people join the organization they have immediate access, as they move roles or projects that new access rights are automatically, and all access is swiftly removed when the person leaves.
- **Access requests and reviews.** Empower end-users to request access to approved business resources, with seamless access reviews for administrators, with full audit trail.
- **Role management and governance.** Create and maintain roles based on similar attribute types for user groups that are relevant and current, with full visibility
- **Access certification.** Continuously check that people have access that is suitable and relevant for their current roles, with processes to right-size access if it is stale, unused, or excessive.
- **Separation of Duties (SoD).** Reduce potential fraud by ensuring that toxic combinations of access are mitigated before they can cause harm
- **Audit and reporting.** Institute capabilities, reports, and KPIs that keep track of historical data regarding access rights, service monitoring, and compliance

However, IGA is notoriously challenging for many organizations to deploy as it touches nearly every person in the organization, every application, all the infrastructure, and every dataset across increasingly heterogenous IT environments. Why deployments stall or fail can be boiled down to three main tenants:

1. **Failing to prepare properly**
2. **Relying on consistently inconsistent data**
3. **Instituting overly complicated and customized processes**

In this Guide we will describe the most common pitfalls that can sink an IGA program, with useful tips and tricks on how to avoid them.

1. Understating the effort needed

Many IGA deployments and programs go wrong because organizations do not go in with their eyes open to the full magnitude and scope of the desired effect of what they are trying to accomplish. With IGA, it is very important to be aware of the fact that IGA is meant to be a program, and not a project.

The distinction is very important, as a project is a single, focused effort, whereas a program is an amalgamation of many projects over a continuous timeframe with a unified goal. However, many deployments go off the rails because they do not consider the broader objectives and key performance indicators of the organization at large.

Gartner states that "Many IGA projects come about because of a production issue, like an audit finding or a data breach, and buying initiatives follow a firefighting pattern, often skipping ideal planning steps. These challenges increase the probability of security and risk management leaders picking a wrong solution that is strategically misaligned with line of business (LOB) and stakeholder requirement.[1]" Because of the 'pants on fire' approach that many businesses take when deciding to undertake IGA, sometimes the approach can be so single-minded that other critical components get overlooked.

Some proper steps that organizations should take to properly prepare for an IGA program and adequately consider the magnitude of work:

- Map out the technology gaps that caused the issue at hand
- Identify the business requirements
- Establish a timeline of checkpoints and identify what success looks like
- Set parameters for who needs to be involved and in what capacity

[1] Buyer's Guide for Identity Governance and Administration (gartner.com)

2. Not involving the right stakeholders

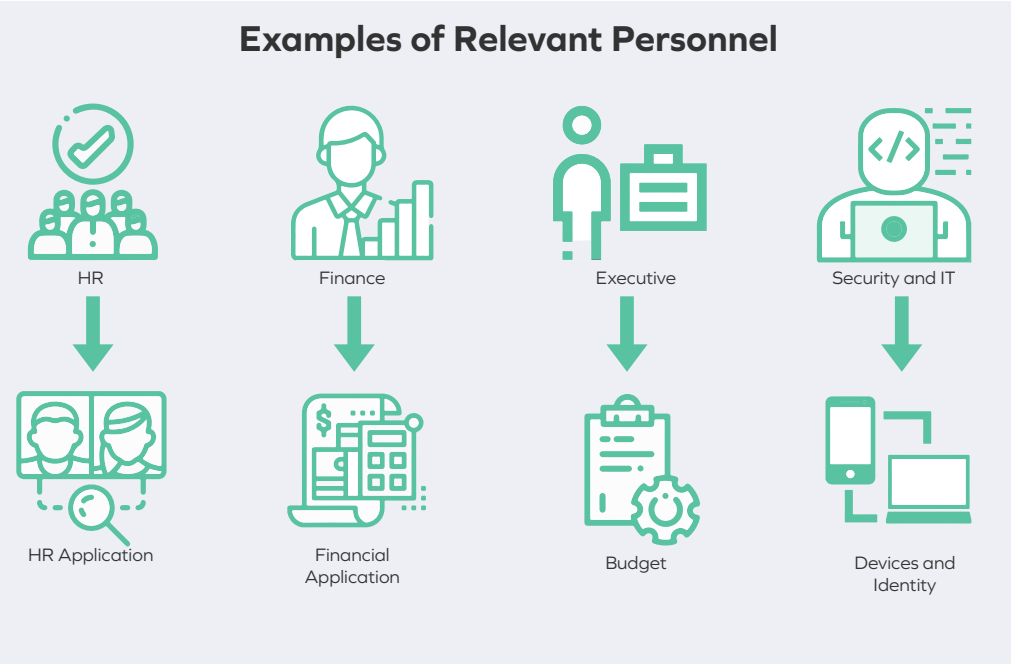
Too often, IGA is considered a technology problem that falls exclusively to IT an the security team to administer and deploy. Typically, IGA will require connectivity to multiple authoritative sources, which can include directory services, HR systems, and more. This inherently requires buy-in from members of all departments, as each respective department will likely have expertise on the functional use of applications that IT simply does not.

This is a common pitfall for IGA programs because of the organizational impact that the tool should have when deployed properly. Without organizational buy-in, IGA tools will fall back to IT to manage, measure, and scale, and will result in stunted growth.

Further, for programs that are technical in nature, it is easy to think that technical people are the only ones who can be trusted to administer the solution. This means enlisting the help of people with Java, Python, or developer skillsets, but it also leads to an inherent shortage of people who can assist in the deployment and scale of the IGA program. Ideally, an IGA solution should be comprehendible for all members of the organization, but minimally invasive in day-to-day operations.

Some steps that organizations should take to properly engage with an IGA solution and ensuring that the right people are involved are:

- Establish all line of business, application, and department heads that need to regularly interact with the IGA solution
- Obtain executive sponsorship, ideally at the C-suite level
- Select an IGA solution that does not require a developer skillset to administer



3. Trying to retroactively clean data

When dealing with identity management and security, often people will have multiple identities, roles, and entitlements that need to be identified, gathered, and consolidated. This data often lives in multiple identity providers (IdP), HR systems, ERP software, and more. Each application has their own way of registering data and can also introduce multiple entries, for instance a title could be entered in one system as “Systems Administrator” another has the same person’s title as “System Administrator” and yet another that has “Systems Administrator II” which can wreak havoc if not fuzzy matched. Many systems also contain duplicate records of people, job titles, projects, and more that can further muddy the water of what is real and what is not.

- IBM estimates that bad data costs the US economy $3.1 trillion each year [2]
- Bad data has a direct impact on the bottom line of 88% of American companies [3]
- Nearly 60% of those surveyed didn’t know how much bad data costs their businesses [4]

Bad data has a direct impact on businesses bottom lines and productivity

This can rear its ugly head with IGA projects and have a snowball effect where bad data is imported into the IGA system from various authoritative sources, which then serves as the foundation for further bad data, leading to misassigned access and entitlements. And so on, and so on. It can also lead to business partner accounts that do not have proper ownership, exacerbate a problem with orphan accounts, over-permissioning, under-permissioning, and general lack of oversight into who has access to what, why, and when.

Some steps that organizations should take to set themselves up for IGA success include:

- Proactively clean data in the source systems, like HR applications, ERP, directory services, etc.
- Identify a process to ingest data in real-time from authoritative sources
- Implement fuzzy matching and leverage a flexible data model to de-duplicate incoming data

2 Journey to AI Blog - The IBM Data and AI blog

3 The Real Cost of Bad Data (intelligent-ds.com)

4 How to Stop Data Quality underminding Your Business

4. Overly granular roles

A key feature of an IGA solution is the ability to assign access rights to groups of people based on their job function, title, department, and so on. However, when implementing IGA, far too many teams focus on the exceptions and not the rules.

This comes from overcomplicating the birthright process by getting away from the very thing that makes role-based access control useful. Ideally, birthrights should be applicable across the organization, and will enable an organization to quickly provision access to a baseline of applications that people need to be productive, and can include email, communication channels, benefits software, and more. However, what it should not include, is anything that is not broadly applicable to people throughout a given role or job function.

Too many organizations are so eager to assign fine-grained access rights and entitlements to each individual member of the organization that they overlook the basics and inadvertently overcomplicate things. This can lead to great confusion from department to department as they comb through granular roles to identify who they apply to (or don't), and massive effort in maintaining roles. Roles, like people, will change as organizational needs change, and can quickly become outdated, particularly if they are over-engineered.

As such, when implementing role management within an IGA solution, organizations should:

- Establish what birthrights should be assigned to the entire workforce
- Implement role-based access control and paint with a broad brush to provide access to people based on their job function, day-to-day responsibilities
- Enable people to easily request access to systems or business resources not assigned out of the box

5 Bayer Implements Omada's IGA Solution

5. Believing "We are different than everyone

It is tempting to buy software, particularly software as a service, and try to bend it to fit the exact specifications of the business. After all, each business does things a bit differently, with different combinations of products they sell, applications they use, whether they deploy things on-premises or in the cloud, where the workforce is located, and more. However, legacy IGA solutions that rely on customization can take extensively long to deploy and point in time solutions simply do not scale as digital transformations take place, workforce needs evolve, and new compliance mandates are introduced.

Setting up bespoke processes may seem like a good idea. For example, each business likely has a unique way of creating new identities when someone joins the organization. But take for instance a large company hiring someone with a common name. The organization might be tempted to customize a process based on their business requirements to accommodate a name, title, email address, etc., but then how that identity gets created in each target system gets more and more complicated. As people with the same name are hired, this could create a problem down the line.

Many IGA workflows should be able to be configured through API calls or through out of the box configurability, but too often, organizations will customize this process leading IAM teams and security leaders to scramble to keep up.

> *"We now have solid processes for recertification and audit permissions that give us full visibility. Our front-end customers can now easily request access and get access to applications quickly leading to significant productivity and time savings."*
>
> – Michael Vogt, Head of DPDC DC EMEA Delivery Center North, DEKRA Group

To properly implement IGA, organizations should seek out standards-based approaches because:

- Allows business to be confident that IGA processes are covered and implemented according to best practices
- Easily prove auditor questions around identities' access to confidential and sensitive data
- Free up administrator time with a configurable approach to IGA, rather than customization

5 https://www.talend.com/about-us/press-releases/gdpr-compliance-rate-remains-low-according-to-new-talend-research/

6 https://www.gtlaw-dataprivacydish.com/2021/09/how-long-do-retailers-take-to-respond-to-access-requests/#edn2

6. Trying to do too much too soon

Many IGA programs do not get off the ground because organizations do not focus on the core tasks at hand and try to jump ahead to advanced use cases. Thinking back to the introduction, with the seven key 'features' of an IGA solution, organizations will too often rush to try to automate everything including leveraging AI and advanced algorithms to automate tasks. This includes the initial phase of connecting IGA to a plethora of applications. With the average organization new deploying 188 applications in production , many try to onboard all applications right away which can slow things down considerably.

This can all lead to a lack of focus on the core tasks at hand, and stall releases and project milestones. Part of it is human nature, everyone is drawn to shiny new objects and wants to handle edge cases like automation and AI. However, many organizations do not get to these advanced use cases because they fail to tackle the basics. Part of this is solved by taking a deliberate and phased approach to IGA.

Here are a few steps to take within a defined period of time:

- Identify the key authoritative sources to onboard identity data from. This would likely include directory and/or HR services
- Categorize the next 'tier' of business-critical applications or systems to onboard
- Deploy IGA with multiple environments that include production, pre-production, and test
- Establish a training program to enable people to administer the solution
- Craft a basic role model with birthrights and assignment policies based on identity attributes

Key Takeaways

There are many reasons for any organization to undertake an IGA program, including boosting workforce efficiency and productivity, enhancing security measures, and meeting an evolving set of compliance mandates. However, how an organization approaches IGA can lead to problems that stall deployments and stunt future growth.

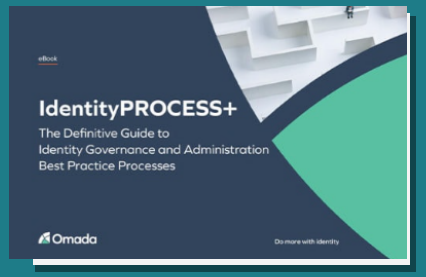
Some things to keep in mind when planning for, and selecting an IGA solution:

1. Be thorough in evaluating all the business needs for identity management and governance
2. Seek and obtain buy-in from leaders across the organization, not just IT
3. Proactively clean data in authoritative sources like the directory and HR system
4. Create baseline roles and groups that can help assign access to people with similar roles and responsibilities
5. Identify areas that can be standardized and built around established best practices, rather than trying to reinvent the wheel
6. Craft a project plan that has manageable checkpoints and create tiers of deadlines that map to business priorities

Omada, a leader in Intelligent Identity Governance and Administration:

Helps customers deploy a full-featured IGA as a service solution within 12 weeks with the Omada Accelerator Package

Lays out how to standardize the key functionality of an IGA program with Omada IdentityPROCESS+.



Omada is a global market leader in Identity Governance and Administration that offers a full-featured, enterprise-grade, cloud native IGA solution that enables organizations to achieve compliance, reduce risk, and maximize efficiency. Founded in 2000, Omada delivers innovative identity management to complex hybrid environments based on our proven best practice process framework and deployment approach. Omada has operations in North America and Europe, delivering solutions directly and via a network of skilled partners and system integrators.

Omada

www.omadaidentity.com | info@omadaidentity.com

12222022