Identity Governance:

The Fundamentals to Avoid Data Breach

intragen

Contents

Overview: Identity Governance and IAM

- **86%** of users have too much access
  (BeyondTrust)
- **74%** of data breaches start with privileged credential abuse
  (Centrify)
- **65%** of companies have over 1,000 stale user accounts
  (Varonis)
- About **80%** of data breaches in 2019 were caused by password compromise
  (IDAgent)

The fundamental "front-door" to protecting access to your organisation's applications and data is a user's identity. Ensuring its confidentiality, integrity and availability is mission critical.

Understanding how data breaches can occur due to poor identity management is key in creating a cohesive strategy for protecting the identity and thus, your applications and data.

Although **Identity and Access Management (IAM)** is often viewed as a single security discipline, there are **three distinct domains** within it, all of which must work in synchronisation in order to "lock the front door". These domains are:

- **Access Management (AM), or Authentication/Authorisation**
- **Identity Governance and Administration (IGA)**
- **Privileged Access Management (PAM)**

From the statistics quoted you can see that there are a number of potential threats that could compromise the security of an identity and be exploited by a hacker to cause data breaches. Hence, having a cohesive IAM policy with an operationally effective IAM solution should be the first part of any security program or digital transformation program. This includes cloud adoption where a zero-trust approach is a must.

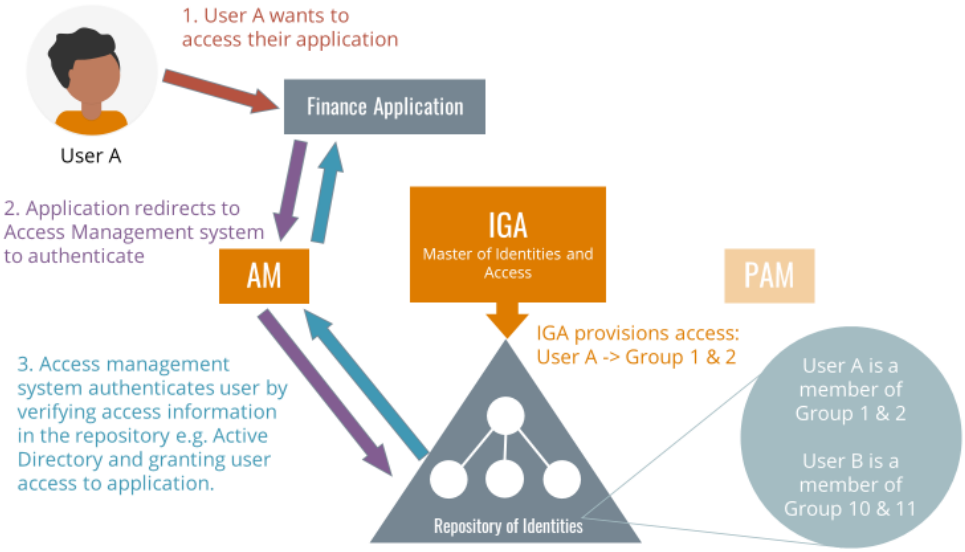
So, how do you determine such a policy or strategy? This can be developed once the end-to-end identity activities are understood.

At a high level, the business activities that an attacker would try and exploit are mundane and every day:

A) A business user trying to access a business application

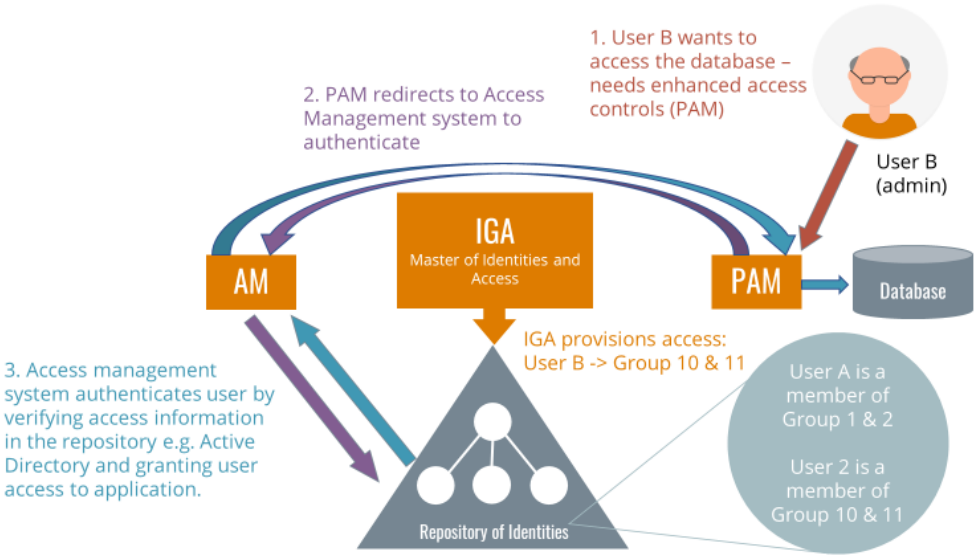
B) An IT administrator trying to access infrastructure such as a database

Case A



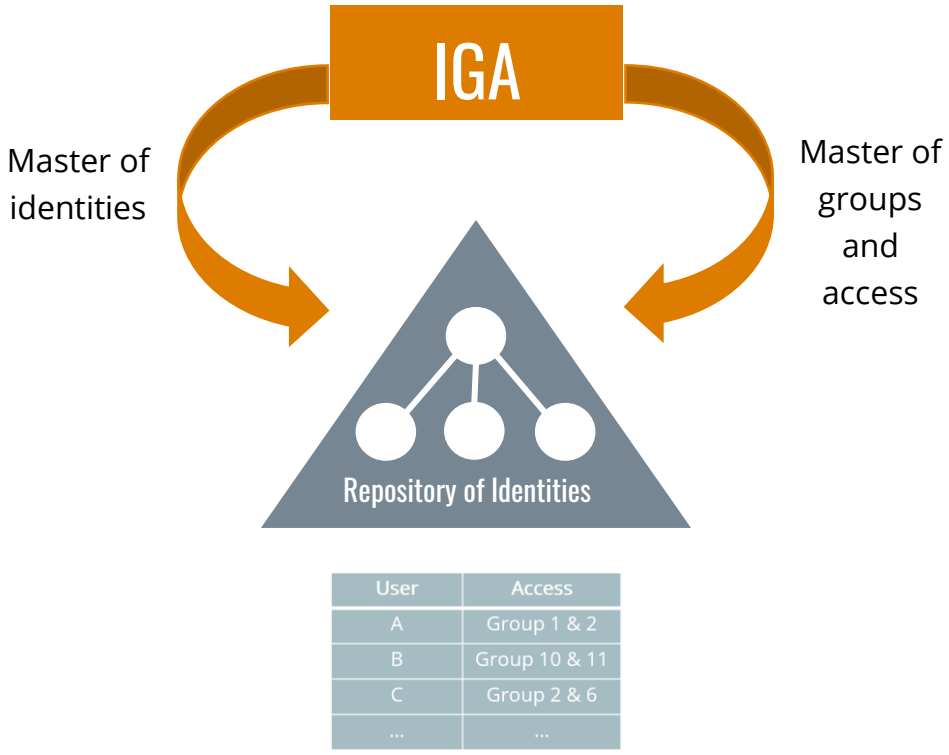
The application first needs the user to identify themselves using some credentials (username, password, fingerprint etc.). This is called authentication. Once authenticated, the user will be checked to see what access level they have, if any, so that the application can give them access to certain capabilities and data. This is called authorisation. Ensuring authentication and authorisation processes are secure is typically externalised by the business application to an **Access Management (AM)** system. This uses techniques like Single Sign-On (SSO) for user convenience and Multi-Factor Authentication (MFA) to minimise the risk of compromising the identity by an invalid party.

Case B



As administrators have "super-user" access to an organisation's "crown jewels" (i.e. direct access to the data or critical infrastructure such as DNS servers, routers and so on), these need to have enhanced access controls. This is the domain of **Privileged Access Management (PAM)** and uses techniques such as break-glass access, credential safes, keystroke recording and session recording to ensure this access is only possible when strictly necessary and that when access is used, it is monitored and often recorded too.

So, where does **Identity Governance and Administration (IGA)** fit in the picture? For both AM and PAM systems to work, they rely on a store that holds the identities with accounts and their credentials for authentication, plus the access level that account has (such as group memberships) for authorisation. An example of such a store would be Active Directory. The account and group information in this store must be 100% accurate, otherwise the AM and PAM systems would all be compromised.



As an example, imagine that the directory contained active accounts for people that had left the organisation or that accounts still had access to applications they needed in a previous job at the organisation, but don't need and shouldn't have in their current job. This is where IGA plays its role. It is the master of identities (and their associated accounts) and their access (group membership), without which other IAM domains are compromised. IGA includes joiner, mover, leaver (JML) access control, access request and approval, provisioning of access and attestation of access as its core use cases. Thus, it is fundamental. It should be the first step towards a cohesive IAM strategy.

The Principles of IGA

Since the IGA system is the master of identities and what access they have, in order to avoid data breaches, there are a set of principles that must be adhered to:

1. Principle of least privilege

This principle dictates that a user is only granted the minimum (least) access required to do their work, for a specific time period, and removed immediately when no longer necessary.

With 74% of data breaches taking place through the use of privileged accounts and 86% of users having too much access, organisations are giving unnecessary privileged access to users. This allows attackers a greater surface area to target their attack. Ensuring people and systems follow the least privilege principle will go a long way to reducing the probability of a data breach.

2. Principle of automation

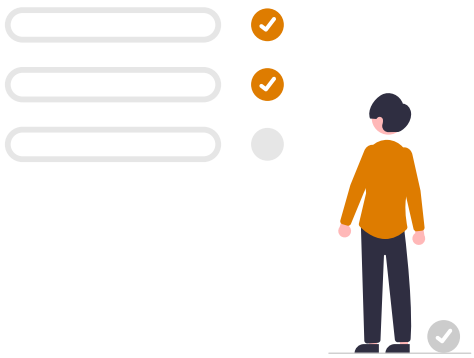
As with many IT disciplines, where there is a manual process, this should be replaced by an automated one. This is even more important in the IGA space. Given the dynamic nature of most businesses today and the fluidity with which people join, move within and leave an organisation – employees, contractors, third parties, etc. – trying to accurately manage their identities and access manually is impossible. However, it's typical to see manual provisioning of access and accounts, leading to organisations open to having active accounts of leavers, who left many years ago.

3. Principle of clarity

In the access control process, the most critical and potentially weakest link is the human element. In identity governance, they are the person that approves or rejects access i.e. they are the true "control" part of the process.

With the best technology in the world, if the person approving access approves inappropriately, then an organisation is increasing the chance of a security breach. Therefore, we need to ensure that the person who is approving that access is also appropriate and has the capability to make the right decision. This means they need to understand what is being requested and why, and determine if it follows the principle of least privilege.

It sounds simple enough, however, this is far from the reality we see. It is common that the approver does not understand what they are approving – there may be little, confusing or no description of the access/group that is being requested, with no additional metadata to understand the risk of approving. This is where the principle of clarity must be adhered to – ensuring that all access is clearly described, and the approver has the knowledge to make a diligent decision. It is important to note this is a labour-intensive task and requires the business to invest in creating high quality descriptions that are understood by IT and business users.



4. Principle of non-repudiation

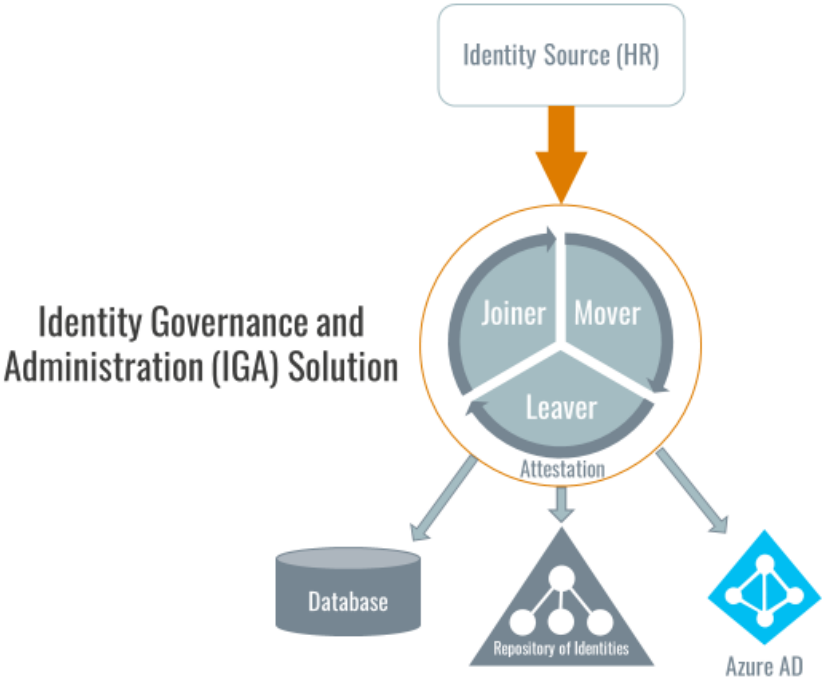
All identities and granting of access must be able to be traced back to an individual unique owner. This requires that all identities have a unique identifier, as should all accounts. It also mandates that each application has an owner, and approvers of access must be defined, each having their own unique identifier. These identifiers should not be able to be recycled to others, regardless of whether the owner of the identifier leaves an organisation. This also supports the next principle of auditability.

5. Principle of auditability

All actions within an IGA system must be audited for compliance and traceability. All actions require timestamps, the subject and person that took the action, the action taken, and the before and after state. This provides the capability to determine the state of a user's access, why something was approved, what triggered the action, and so on, at any point in time. It is common that these audit trails are used or required by auditors or an operations team if there has been an incident.

IGA Use Cases and Best Practices

IGA covers many use cases, with new ones being defined in the domain on a regular basis. This chapter will cover the core use cases that it must address - the minimum that are required for an effective identity governance solution.



Core Use Cases:

- Joiner, Mover, Leaver
- Access, Request and Approval
- Attestation
- Role-Based Access Control

Joiner, Mover, Leaver (JML)

JML processes are the controls that manage the lifecycle of an identity, ensuring that it maintains the principle of least privilege.

> **Best Practice Hint**
> Create the identity and associated accounts in a disabled state prior to a new user's start date, and only enable when the user joins – setting up access before but keeping accounts locked down.

The IGA system starts with a source of human identities from an HR system for example. An aggregation layer can be created for multiple sources of identities, such as systems for third parties, so the IGA system only has a single feed. The HR system provides the source of data that will drive the JML workflows. Accounts and access via group memberships should automatically be provisioned, ideally based on a template (or role) that is defined for each user type. However, manual approval steps can be included according to business needs.

> **Best Practice Hint**
> Your IGA system will only be as accurate as your HR system – ensure you work closely with your HR colleagues to create an accurate and timely upstream data source.

Mover events are important to manage insider threats – the reason why so many organisations have people who are over privileged is that as they move around an organisation they take their access from one job to the next. When someone changes job there should be re-validation of their access to ensure it is necessary in their new capacity, and anything else should be removed.

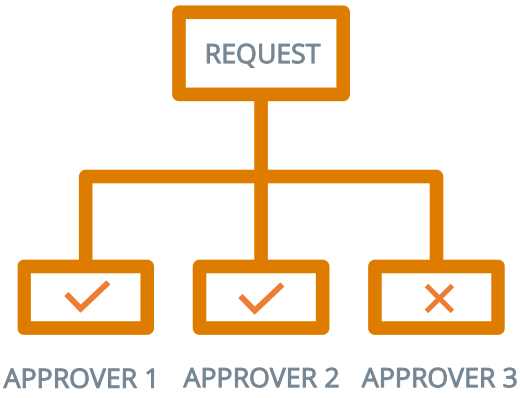
Leaver processing is a low hanging fruit to remediate a large threat vector. An organisation should have at least two workflows to manage leavers – the standard workflow and emergency termination workflow. The standard automated workflow should be triggered by an expected HR termination event, such as retirement or "good leaver". The emergency termination process can be manually triggered by someone such as the line manager to deal with emergencies such as a "bad leaver".

Access, Request and Approval

In order to ensure that the IGA system is the master of all approved access, all access requests should be made via the IGA system. The first step, following the principle of clarity, is that you need to determine how to define and structure access. Ultimately, this access will result in a group membership in some security store such as Active Directory. But the IGA system gives the ability to abstract that and provide additional metadata so that the people requesting and approving access can both have clarity on the access request. Define your application and its access rights (which will be provisioned as groups) with clear ownership, descriptions and risk information. After this, you can specify the approval workflow and who the approvers should be.

Best practice hint

Always ensure the line manager is the first approver, as they know the "who" and the secondary approver to be the business application owner, who know the "what" is being approved.

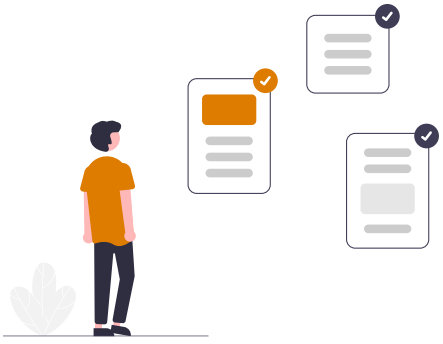


Attestation

Historically, especially within the finance sector, before the formal concept of IGA was coined, attestation or recertification of access was the primary mechanism used to ensure people had the appropriate access. Attestation is a period review of someone's access – a snapshot, which is reviewed on a regular basis – annually, quarterly, or even more frequently. It continues to be an important part of IGA as a catch-all, confirming appropriateness of access, regardless of whether an individual has gone through a JML event or not.

Best practice hint

It's important to follow the principle of clarity for attestation. Given it may be used to collect access data from a variety of sources, the quality of descriptions and names may be low, so clean them up! Ensure that a single person doesn't have too many things to review – they will be overwhelmed and treat it as a tick-box exercise.



Role-Based Access Control (RBAC)

Most organisations will have hundreds or thousands of access rights to their applications and infrastructure. For an end-user trying to request them or an approver who has to review them, the volume can swamp them with too much information, leading to incorrect requests and too many approvals. RBAC can be used as a way of defining a collection of access rights, which are related in some way. For example, a role may be defined for a financial advisor. This role can be requested once and give access to multiple applications. In this example, underneath the covers the financial advisor role would be composed of say “accounts_uk”, “loans_products_readonly”, “financial_reporting”.

Defining roles for an organisation is not always an easy task and requires analysis of the best way of grouping access rights – which may not easily map to a specific job type. The advantages for a requester or approver is that they will see a single role rather than say five or ten individual access rights.

RBAC supports the principle of clarity and automation by more clearly and easily defining access and reducing the volume of requests that require approval, facilitating a more diligent decision.

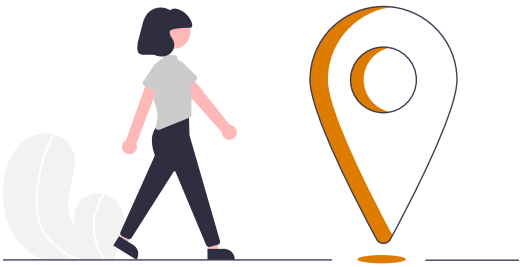
Other Use Cases and Best Practices

As you continue to improve the management of identities and access, numerous other use cases and best practices could be considered. This includes topics such as segregation of duty (SoD) controls, attestation of role content, and the use of machine learning to determine approval rules and risk level, to name a few.

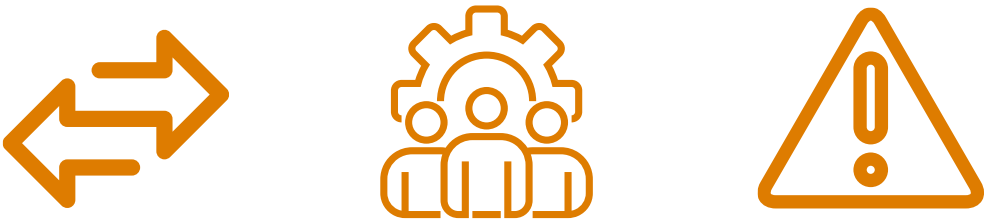
However, that would be the subject of a different set of papers!

Best practice hint

Get the fundamentals right before looking at advanced topics – layered IGA security is the right approach.



Solving the IGA Puzzle: Transfer, Manage or Accept the Risk?



Having understood the importance of IGA, and the typical use cases and challenges in this space, how best do you implement an IGA solution?

Our approach at Intragen is taking the risk model approach of either transferring, managing or accepting the risk.

In today's digital, open and interconnected business models, where data is the real asset and customers understand the value of their data, accepting this risk is not one we commonly recommend.

This leaves the possibility of either **transferring or managing the risk**.

Transferring the risk to a third-party provider of, for example, a SaaS solution is a valid option. Although you will always be accountable for the risk, it allows you to transfer it so it can be managed outside your organisation.

Managing the risk requires that you own and manage the risk on a day-to-day basis and implement an organisation-specific solution. This enables you to have better control over the risk, but with higher investment.

Intragen provides solutions for both approaches.

For the **transfer** option, Intra1 - www.intragen.com/intra1 - provides an Identity Governance-as-a-Service cloud-based solution. It allows organisations with minimal or no IGA experience to set up all the fundamental use-cases described in this document in days rather than months, with all the best-practices built in. This approach works for relatively standard cases described here and fulfils the requirements of most organisations. To find out more, click here.

Where an organisation wants to **manage** the risk, the focus is on a tailored solution. Intragen has been implementing IGA solutions since 2006, with well over 400+ successful implementations.
Using this experience, and our implementation accelerators, we can quickly understand your business problems, assess your current status and create and implement a roadmap to achieve a secure target state. For more information click here.


intragen
SECURING YOUR IDENTITY