eBook

IdentityPROCESS+

The Definitive Guide to Identity Governance and Administration Best Practice Processes

Omada

Foreword

Most organizations today are operating in a hybrid IT environment of on-premises and cloud-based applications, which make it difficult to get transparency on who has access to which IT systems and applications in an organization and why. Identity Governance and Administration (IGA) has become a cornerstone of solid IT security, allowing organizations to implement processes for controlling, managing, and auditing access to data, which is an important prerequisite to reduce the security risk.

Over the past 20 years, Omada has built up a body of knowledge from a significant number of IGA deployments in some of the world's largest enterprises as well as in many medium sized businesses. This expertise has been formalized into the unique IdentityPROCESS+ best practices process framework, which sets out the process areas needed to design and implement a successful identity management and access governance solution.

In this book we use the abbreviation 'IGA'. It is the term Gartner; a leading analyst company uses in its 'Magic Quadrant for IGA (Identity Governance and Administration) report' as well as the Critical Capabilities for IGA report. To add to the confusion, Gartner's IGA scope is a combination of the scopes of the two previous Magic Quadrant market research reports covering identity and access management (IAM) and identity and access governance (IAG).

Our framework scope encompasses all processes used to manage identity and access controls across systems. The IdentityPROCESS+ framework covers the scope included in Gartner's IGA definition and more. So, although we should probably have called our scope IMAG 'Identity Management and Access Governance' we have chosen to use the term IGA for simplicity.

This book aims to inform CISOs, Security Managers, IT Directors, and those with direct or indirect interest in cybersecurity how adopting the IdentityPROCESS+ framework will help them successfully deploy and maintain an IGA solution to realize the security, compliance, and efficiency benefits they need to run their business.

The first chapter provides:

- An overview of the challenges organizations face when looking to embrace digitization to gain a competitive advantage
- An introduction to the different aspects of IGA
- An overview of the potential challenges related to implementing IGA projects
- A high-level summary of the IdentityPROCESS+ best practice process framework and an introduction to the seven process areas that make up the IdentityPROCESS+ framework

The first chapter explains how implementing best practice processes helps organizations manage identities and access rights throughout an employee's career, ensuring good governance, managing user access in hybrid IT environments, aligning identity management with the business, and protecting critical digital assets before and after a potential breach has been identified.

In chapter two, the process areas are examined in more detail to provide a greater technical-level understanding. The operation of each process is explained in detail along with implementation best practices, key stakeholder involvement, pre-analysis questions, and key recommendations.

After reading the book, IT security professionals and business leaders with an interest in security and compliance will have a good understanding of how adopting the best practices framework will help to secure a successful IGA project.

Acknowledgements

The IdentityPROCESS+ framework is based on experience gained from thousands of work hours by Omada consultants, partners, and customers - continuously developing, refining and deploying IGA processes. We would like to thank everyone for their collaboration and feedback. The input from organizations across all market verticals has proved invaluable to making IdentityPROCESS+ a robust framework on which organizations can build their future IGA deployments. We will continue to develop this industry standard framework that goes hand in hand with the built-in processes and the approach in the Omada platform which automates the best practice IGA processes.

Find out more

To learn more about implementing the processes in IdentityPROCESS+ in your organization, please contact Omada at info@omada.net

Content
IdentityPROCESS+

CHAPTER 1

CHAPTER 2

Introduction
The Journey to IGA

Organizations of all sizes and across all industries are using more and more on-premises and cloud technologies to be effective and increase efficiency to remain competitive in the markets they operate in. In doing so, organizations reduce costs, increase productivity, and minimize the time-to-market of their products. However, while digitization provides significant benefits, it can also pave the way to unwanted challenges which broadly speaking can be divided into three main areas:

LACK OF ADEQUATE SECURITY

Organizations struggle to secure that all IT systems – onpremises and in the cloud meet strict identity and access security requirements to avoid security breaches

NON-COMPLIANCE

Organizations find it difficult to enforce identity and access governance policies and perform mandatory procedures to ensure that all IT systems and services meet internal and external regulations

MAINTAINING EFFICIENCY

Organizations are challenged with the need to avoid excessive workload on already stretched IT staff as the organization grows through hires and M&A activities and as new IT systems are added continually to their portfolio

If these challenges are adequately addressed, organizations can obtain the benefits that current IT systems and new technologies offer while simultaneously increasing efficiency and competitiveness without compromising security. Before delving into the best practices that help organizations manage identities and govern access to meet the above business needs, it is necessary to explore common business challenges to put these challenges and consequent needs into context.

LACK OF ADEQUATE SECURITY

Security breaches have far-reaching consequences

Far from being just an inconvenience to the organization, security breaches caused by insiders or external attacks can result in a severe impact to business operations. The insider threat from employees and contractors, and external attacks can be both unintentional or malicious, but either way, the effects of the security breaches are the same, including loss of productivity, corrupted business data, significant clean-up costs, stolen intellectual property, reputational damage resulting in loss of customer or partner trust, and fines and litigation for not complying with national or international laws.

Consequently, security is no longer just an IT matter, but a board level concern. Without the appropriate board-level sponsorship, organizations risk embarking on projects, which have inadequate attention or funding, or fail to cover all the necessary areas of security.

Security and the process of governing identities and access

Organizations are realizing that enforcing the right processes for governing identities and their access is key to ensuring adequate security, for instance in connection with the procedure for locking down access correctly and in a timely manner in case a security breach should occur.

The value of best practice standard processes

By implementing best practice standard processes for identity management and access governance, organizations assure that they cover all security aspects related to identity governance and administration across hybrid IT environments, allowing the business to be confident that processes are covered and implemented according to best practice.

ADDRESSING NON-COMPLIANCE

Compliance with laws and regulations is essential

In addition to the pressures that cybersecurity requirements place on businesses, most organizations find that being compliant with a wide variety of regulations is increasingly important. Whether it is the Sarbanes Oxley (SOX), Bafin, General Data Protection Regulation (GDPR) affecting all companies with European customers, the Australian Privacy Act, California Consumer Privacy Act (CCPA) or the many other laws and regulations that affect data privacy, organizations need to ensure that they can fulfill their obligations. Compliance requirements include controls and logs of access approvals and access history for audit purposes. For many businesses, the ability to prove compliance is essential to maintain an operating license, for instance within the banking and finance sector.

The business' "License to Operate"

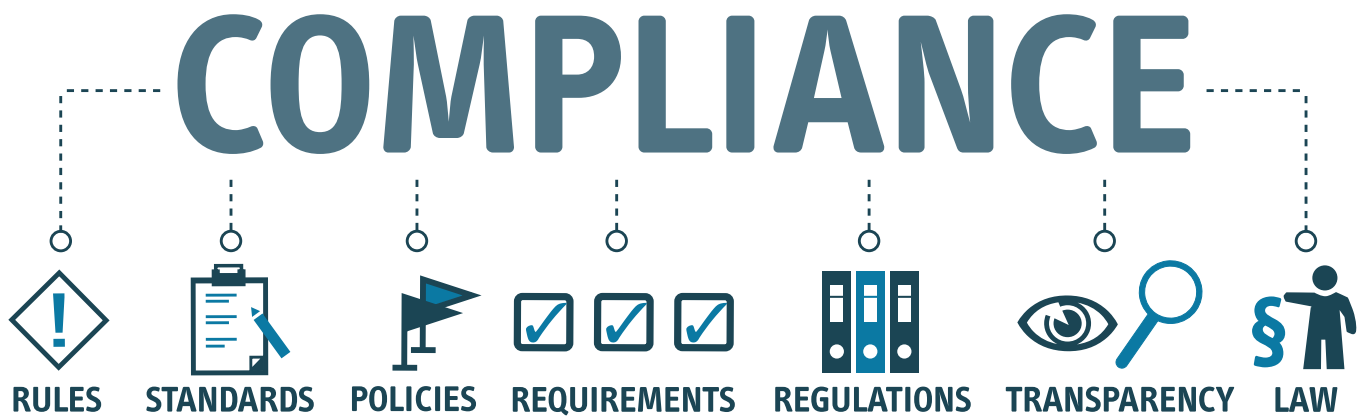
In the GDPR era, compliance has become a 'License to Operate' for all organizations. It is imperative that organizations can prove that identities and their access to data are documented and treated according to best practices and high standards. On top of this, many organizations decide to prove to customers, business partners, and governing authorities that they are adhering to specific security policies such as those defined by ISO27001 or similar. A lack of compliance evidence can lead to lost contracts, both on the customer and supplier side, as it is perceived to be risky to conduct business with an organization that has inadequate data handling processes. This means it has become a competitive advantage to reassure customers and business partners that appropriate action is being taken to protect data and maintain a high level of security.

Compliance and the process of governing access

Governing identities and access is of paramount importance in terms of being compliant with GDPR and many other laws and regulations. The ability to document that best practice processes are followed is vital in audit scenarios as inspectors need to be reassured that an organization has control over who has access to what. If businesses can demonstrate that policies, procedures, and technologies are in place to govern access, control identities, and report on any violations, they are more likely to meet the requirements set out by various regulations.

The value of best practice standard processes

By implementing best practice standard processes, organizations can prove they have the necessary access governance controls in place, satisfying auditor questions around identities' access to confidential and sensitive data, such as financial information or privacy data.



MAINTAINING EFFICIENCY

Vital to maintain efficient operations

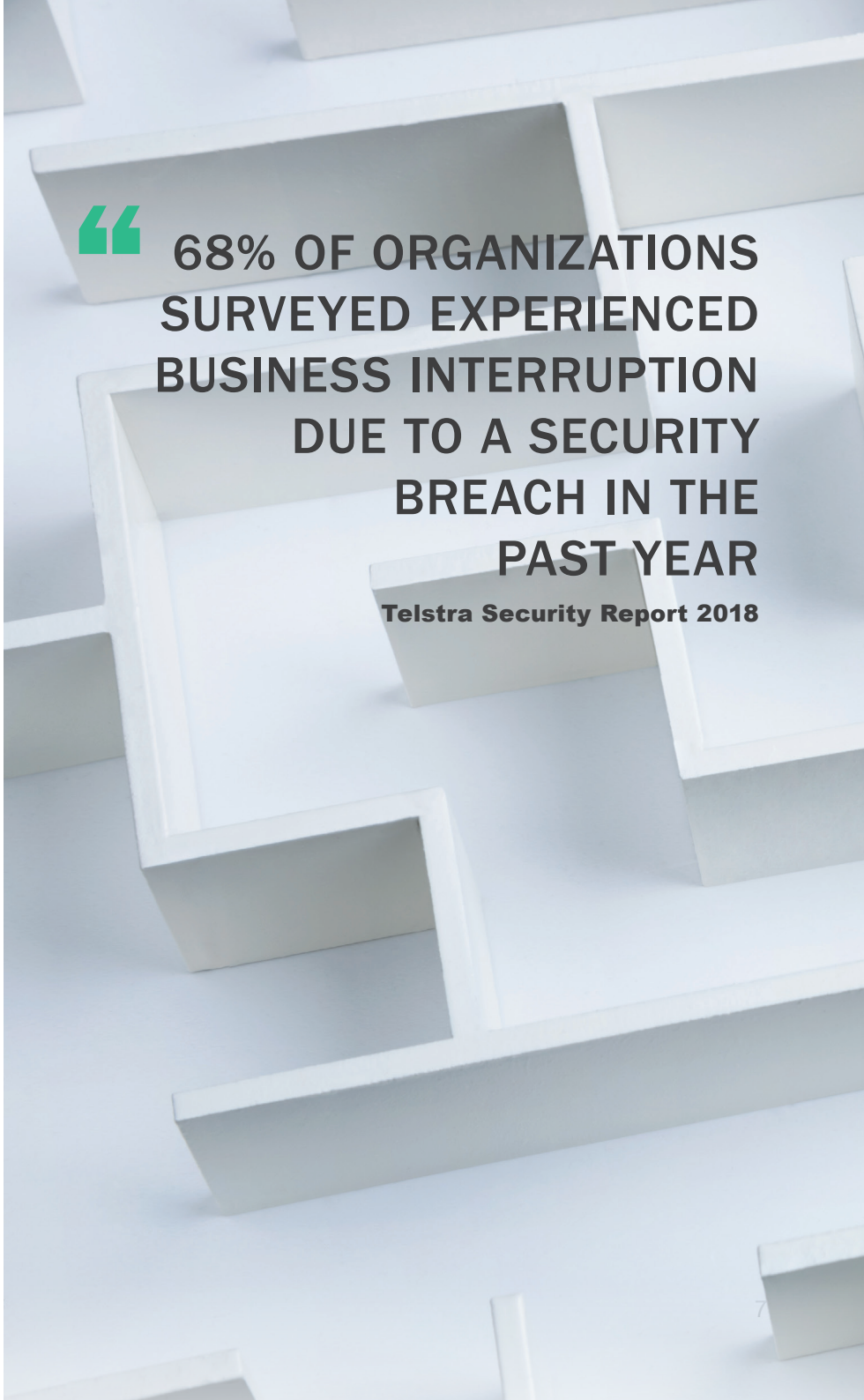
When organizations grow and add new systems (cloud or on-premises), process increasing amounts of data, onboard and off-board employees, partake in M&A activities, or grow their network of business partners, they must acknowledge the significant resource implications this requires.

Efficiency and the process of governing access

The process of governing identities and their access promotes cost reduction by streamlining identity lifecycle processes such as onboarding, off-boarding, and departmental changes for employees, business partners, contractors, and customers. By establishing processes for governing identities and their access, organizations warrant significant time-savings, as processes such as access reviews and certifications as well as access request and provisioning of access rights are simplified.

The value of best practice standard processes

Implementing best practice processes for improving the handling of users, identities, access policies, roles, and controls ensure that you are working in an efficient manner giving employees, managers, and business system owners more time to deal with more value-adding work.



> 68% OF ORGANIZATIONS SURVEYED EXPERIENCED BUSINESS INTERRUPTION DUE TO A SECURITY BREACH IN THE PAST YEAR
>
> **Telstra Security Report 2018**

Identity Governance and Administration

The Essence

Securing the right access to the right individuals

Ensuring that employees, contractors, third-party vendors, customers, and Internet-of-Things (IoT) only have the right level of access to the systems, applications, and data they need to do their jobs or to interact with the company, is important to run a secure, compliant and efficient business. Within the IT department of a company, this discipline is referred to as identity governance and administration (IGA).

IGA processes provide compliance, security, and efficiency

An IGA solution allows an organization's IT department to manage and govern all user access rights across a hybrid IT environment of on-premises and cloud-based enterprise systems.

IGA processes include managing access to resources across an organization's hybrid IT environments (on-premises and cloud-based applications), audit and compliance reporting to ensure continuous risk overview, onboarding of new employees, performing access reviews and certifications across all cloud and on-premises applications, a structured approach to onboarding applications, and managing access to applications on a granular level in compliance with company policies, handling of access assignment policies and provisioning.

Being able to effectively process these elements allows organizations to save costs, ensure compliance, and minimize the risk of data theft by insiders and hackers. A key factor in doing this, is ensuring that business systems are only accessible to those who need to use them to do their job.

Businesses need IGA processes in place to ensure security, compliance, and efficiency, protecting organizations from incidents that could damage the reputation or, in the worst case, cause them to go out of business. In today's cloud era, with soaring security threats and hard-hitting legislation such as GDPR, having best practice IGA processes in place has become a license to operate.

Deploying an IGA solution should be seen as a strategic investment, empowering organizations to realize significant business value across the organization.

Reap the Benefits

The key processes of identity governance and administration provide distinct business benefits.

SECURITY

- ✓ **Protect your image and reputation**
  Prevent data leaks by minimizing access to sensitive data and business critical IP and limit the consequences of a security breach by having an optimized process for suspending compromised accounts in case of security violations.
- ✓ **Protect your data and IP**
  Achieve a 360-degree overview of all identities and access rights across hybrid systems and applications and control that users have the correct access in compliance with policies and regulations. Minimize risks by automatically identifying orphan or inactive accounts, that could be misused for attacks.

COMPLIANCE

- ✓ **Enforce compliant policies**
  Enforce and document adherence to access policies across all applications and systems. Policies include segregation of duties (SoD) policies, role-based policies and policies as defined in SoX, HIPAA, CoBIT, EU GDPR, ISO27001, BaFin, CCPA, and other frameworks.
- ✓ **Establish access compliance processes**
  Establish processes for handling of security violations by continuously monitoring current access state in comparison with target state and carry out mitigating actions on demand.

EFFICIENCY

- ✓ **Increase productivity**
  Streamlined onboarding processes save time as employees or contractors get access to the systems, they need to do their job from day one. Manage access as the employee changes roles in the company and revoke the access across platforms when access is no longer needed.
- ✓ **Free-up valuable time**
  Achieve significant time-savings for managers, internal auditors, system owners, help desk staff and other employees by streamlining processes such as access reviews and certification processes (attestation), generating audit-ready reporting for recurring compliance audits.

Avoid IGA Project Pitfalls

IGA projects can be particularly challenging when compared to more traditional projects due to over-engineering and implementation of unproven and flawed processes. Beware of the following:

UNDERESTIMATING THE NEED TO GET ALL STAKEHOLDERS ON-BOARD

There are numerous stakeholders associated within an IGA implementation project including:

- The CISO and their IT security staff who are responsible for the overall security of the IT infrastructure
- Business application owners who want to control access to the systems they manage
- Compliance officers and intellectual property controllers who need to ensure that access to business-critical systems is limited to only those who need it
- Managers of teams who need to ensure that each team member has access to the right level of information at the right time
- Internal auditors that need a transparent access rights overview

Underestimating the need to get these various stakeholders onboard early in the project can lead to delays and poor adoption.

FAILURE TO ADOPT BEST PRACTICES

Companies deciding to stick to old ways of doing things to avoid upsetting the status quo can end up with inefficient processes that do not meet future compliance requirements and do not provide the business agility needed. From an IGA system perspective, failure to adopt best practice processes might lead to unnecessary and complex customizations of a product.

OVERLY AMBITIOUS "BIG-BANG" PROJECT PLANS

Trying to be too ambitious by attempting to implement everything in the initial business case in the first phase rather than identifying and delivering value early and often can lead to unnecessary resource expenditure and poor adoption within the organization.

UNDERESTIMATING THE WORK TO IMPROVE DATA QUALITY

The data related to employees, contractors, third-party business partners, and customers and their access is often stored in multiple systems such as different databases and spreadsheets across disparate cloud-based and on-premises systems. Such data - including authoritative source (HR) data - is often not in a good state. Capturing, normalizing, correlating, and processing this data can present technical, political, or legal challenges and be time-consuming.

Underestimating the work to get data quality right (e.g. to obtain information from line managers to correlate user accounts with actual employee and contractor ID's) might lead to significant delays in a project.

Introduction
IdentityPROCESS+

IdentityPROCESS+ is a comprehensive, best practice process framework, which describes the most important processes needed to ensure a successful IGA deployment. The framework has been developed with the goal of supporting successful IGA projects for organizations worldwide and has been created to help organizations implement well-proven best practice processes, reducing the need to ‘reinvent the wheel’.

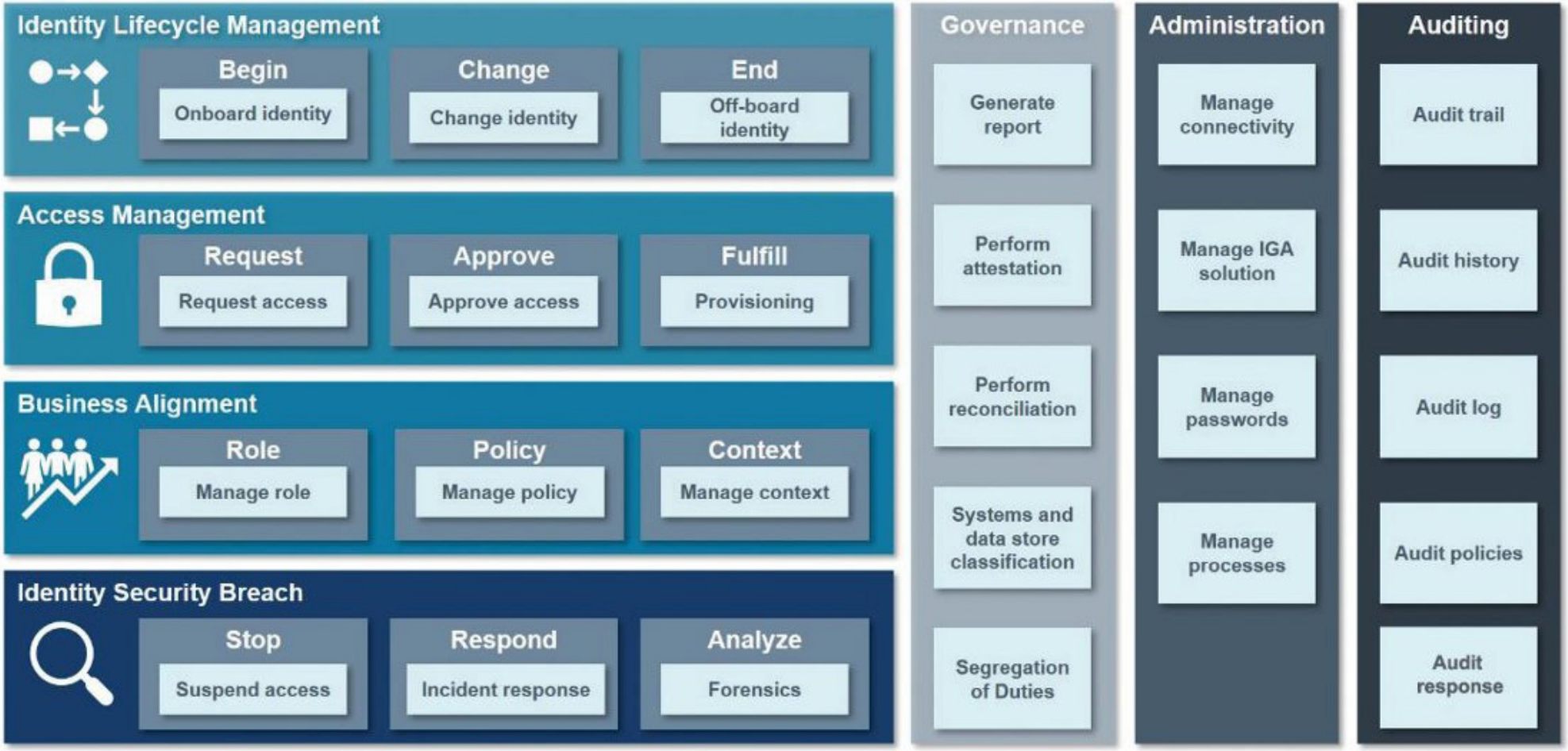


Fig. 1: The built-in processes of the IdentityPROCESS+ framework

IdentityPROCESS+
Set the Vision

The IdentityPROCESS+ framework enables organizations to set the vision for the IGA project and to achieve the planned benefits. Adopting the framework means that organizations significantly increase the opportunity for a successful IGA project.

DIFFERENT NEEDS FOR DIFFERENT STAKEHOLDERS

To achieve buy-in from each stakeholder type in the organization for an IGA project, it is important to be able to articulate and quantify business benefits and visualize the associated business processes and the value they provide. IdentityPROCESS+ helps organizations in mapping business benefits to business processes at an early stage and helps secure alignment and avoid misunderstandings.

The benefits of IdentityPROCESS+ include:

- ✓ Achieve easy deployment of best practice processes
- ✓ Document that best practice identity and access related controls are in place to satisfy auditor questions around access to confidential and sensitive data such as financial information or privacy data
- ✓ Implement best practice processes for streamlining the handling for users, identities, access policies, roles, and controls
- ✓ Ensure that an organization covers all security aspects related to identity governance and administration during a project so that the business can be confident that processes are covered and implemented according to best practices
- ✓ Manage multiple stakeholders by breaking down the entire IGA project into smaller phases making it easier for the project team to visualize and demonstrate the business benefits to other departments
- ✓ Visualize business processes and expected results early in the project so that stakeholders understand the benefits of deploying the processes
- ✓ Achieve organizational alignment as it is easy for non-technical users to get involved in the project
- ✓ Avoid the risk of being overly ambitious by attempting to implement everything in the initial business case rather than identifying quick wins and delivering value early and often
- ✓ Avoid complex customization if/when an IGA solution is implemented, as best practice is known
- ✓ Validate automation of solutions against best practices developed from experiences gained from many thousands of hours of work by skilled professionals
- ✓ Remove the friction that a deployment of a new IGA solution could introduce if not managed properly

IdentityPROCESS+ breaks down the processes included in an IGA solution scope into the seven core process areas, each of which covers one key part of an entire IGA scope. Each of these process areas include process groups, which include a range of processes. These pre-defined processes cover all major processes that must be implemented by organizations to manage identities and perform access governance.

IDENTITY LIFECYCLE MANAGEMENT

A key element of managing identities is the joiner, mover, leaver concept, which manages employees' access rights as they join the company, move department or change roles, and leave the company. Manual handling of these changes is both time-consuming, costly, and error-prone. As a result the company may be exposed to unnecessary risks in case individuals are being granted rights to systems that they should not have permission to access. Identity lifecycle management involves processes that manage an identity through each of these stages.

Onboard identity

It is important for an organization to ensure that the initial join process is efficient so that a new employee is productive from day one with access to all the necessary systems to do their job. Otherwise, their first few days of employment could be wasted on waiting for access to systems. A similar process to onboard contractors and setting up technical identities, or non-personal accounts, is also defined in the IdentityPROCESS+ framework.

Change identity

Throughout the employment lifecycle, employees often change roles, get promoted or move departments. A new job role will typically require additional access to systems already in use or access to new systems. It is not only important to grant the new access, but it is just as vital to ensure that any access rights the employees no longer need are revoked. If this does not happen, then an employee will accumulate more and more access rights over time. This could result in a user having rights which violate company policies such as segregation of duties and increases the risk of data breaches occurring if their account is compromised in case users have access to a larger number of systems than necessary which is valuable to an attacker.

Off-board Identity

When an employee or contractor leaves the company, their access to all business systems and applications needs to be terminated so they can no longer log into the company systems. The termination process handles the off-boarding of an identity of a leaver and is an essential step in securing your organization.

ACCESS MANAGEMENT

A key part of improving the efficiency of identity management involves making sure that end users can request access and managers can approve access to digital resources needed as quickly and efficiently as possible.

The access management processes within the IdentityPROCESS+ framework make it easy for end users to request access to a resource such as a shared drive or a business application. The access management workflow routes the request to a designated manager, who can approve or refuse access.

Request access

Efficient access management improves employee productivity as employees can request new access rights as soon as a business situation dictates that it is necessary for them to have additional access to perform their duties. This process area describes processes for Self-Service Access Request to replace labor intensive and inefficient manual work by unifying access request processes.

In addition to approving/certifying system access, ad hoc and periodic attestation processes shall be conducted. These processes verify that employees and contractors still need access to certain resources. This in turn ensures that employees and contractors do not acquire a greater amount of access rights than they need and that contractors do not maintain access long after they have left the company (see the section on Governance for more details).

Approve access

Contains various processes for single and multi-level approval workflows. The access management processes also include removing user access either after an expiry date has been reached or when it is revoked by a manager or administrator.

Provisioning

This process area includes processes for automated provisioning and de-provisioning of users' access, utilizing policy-driven access rules and defined roles. Automated provisioning and assignment of access rights via rules and policies enables quick roll out of access to new business applications.

BUSINESS ALIGNMENT

User adoption of an IGA system relies on the system being relevant to the company and as easy to use as possible. To ensure this, the IdentityPROCESS+ framework uses roles, contexts, and policies to accurately model the organization.

Building the right, fit-for-purpose models for different roles, assignment policies, constraint policies, and context administration results in a significant optimization of the IGA system which helps organizations realize the identified ROI benefits in the early stages of the project.

Roles

Roles describe users who have the same or very similar jobs. Examples of roles include a sales rep, accountant, programmer, or a project manager. Roles are used to assign users with the same access rights to business systems when they join the company or move to different roles.

Without roles, it would be necessary for all the access rights for each user to be created individually. In organizations with many users the complexity of assigning access rights manually and individually is a resource intensive and error-prone task. Provisioning access rights by simply copying the access rights of existing users, presents another issue. Inappropriate rights may inadvertently be granted to a new employee as the profile of an existing employee in a similar role, may have excessive access rights due to their tenue with the company.

Roles are used to define access rights restraints such as segregation of duty. IdentityPROCESS+ defines processes for role lifecycle management.

Contexts

Contexts allow organizations to model and govern advanced organizational constructs such as matrix management structures or organizations where employees have multiple organizational affiliations.

Like roles, contexts make managing groups of users easier as they can all be treated as a single entity. However, they are different because the member of the group is not necessarily based on the common role of the employee but on the business situation.

Context management processes within IdentityPROCESS+ allow for the fact that people can be part of multiple project teams or can be assigned to temporary assignments in addition to their normal job role. Specific entitlements can be associated with the context. For example, a context could be a department, project, cost center, or building. These processes also support governance of organizational contexts throughout their lifespan.

Policies

Policies cover a wide range of governance requirements within an IGA scope including segregation of duties, assignment of access rights, and data classification. Policies can be assigned to individual users, contexts, or roles and are required to automate compliant access policy handling as defined in internal policies or external regulations like SoX, HIPAA, CoBIT, GDRP, CCPA, ISO 27001, and BaFin.

Assignment policies are used to ensure that assignment of access for identities complies with internal rules and external regulations.

IDENTITY SECURITY BREACH

In the event of an incident where an organization suspects a breach, the security team may want to suspend access to one or more identities immediately to prevent the lateral spreading of the breach.

The identity security breach processes in IdentityPROCESS+ provide an emergency lockout description which enables the administrator to disable a user's access to all on-premises and cloud-based systems.

Limit breach exposure

This cross-system access suspension limits the company's exposure to further breaches while an investigation is carried out and the user's passwords are reset. An emergency lockout can be triggered using the automatic incident response process or manually carried out by an administrator.

If an administrator determines that there has been a breach, the administrator can perform a manual emergency lockout and provide a reason for the lockout which will serve as evidence in future security breach investigations and audits.

To ensure that the identity security breach processes are used correctly, it is recommended that a formal written policy is created. The correct implementation of these processes is discussed in the specific chapter covering identity security breach processes.

GOVERNANCE

Once access has been granted to individuals based on a given set of criteria driven by internal policies and external regulations, continuous attestation or verification is important to ensure that the original justification for the access is still valid.

Being able to stay in control of and prove who has access to which resources, why they were granted access, and who approved the access is important for all organizations that need to stay compliant with internal security and compliance policies as well as with external regulations such as GDPR, CCPA, and ISO 27001.

The governance processes within IdentityPROCESS+ enable organizations to:

- Enable managers / system owners to attest on an ad hoc or scheduled basis whether access rights for identities, types of employee, or contexts are still valid
- Generate reports showing policy violations such as segregation of duty conflicts
- Provide reports such as the actual status of access across all enterprise applications to satisfy audit requirements
- Request system owners to classify business systems that contain classifications of data which needs special treatment – for data that falls under specific regulations, or confidential data that needs appropriate risk controls applied
- Report policy violations, who approved them and the business reason why they were approved

The governance processes help organizations to keep in control of and report on who has access to what as well as why the access was granted. This allows organizations to maintain high levels of security, efficiently identify and address policy violations, and save licensing costs when employees are no longer using software.

ADMINISTRATION

Over time, companies deploy new business systems to match changing business requirements. It is important that these new applications are connected to the IGA solution so that access to them can be managed and governed efficiently.

The administration processes within IdentityPROCESS+ allow:

- Efficient onboarding of new systems and applications
- Applying meaningful descriptions for resources to make it easy for end users to find resources when making self-service requests
- Performing application management
- Setting up the password reset management and password policies

The administration processes make it easy for identity administrators to oversee the applications that are being managed or need to be onboarded. This allows administrators to spend time focusing on ensuring appropriate access to applications rather than on integrating new applications and performing other routine tasks.

AUDITING

As technology evolves within organizations, compliance has become a more complex topic that has the attention of executives and senior management. Internal security requirements and polices combined with regulatory legislation can lead to increased complexity. The ability to audit has become a focal point for organizations to control and monitor access to intellectual property and data while at the same time provide reports with detailed information about access policies and user permissions in order to maintain and document compliance.

Organizations that leverage their IGA solution to enforce business rules and policies, mature their audit process. By transforming manual auditing processes to a more mature automated model, they can significantly reduce the time and cost involved with compliance reporting. This is an essential element for establishing the foundation for an Information Security Management System (ISMS).

The ability to continuously monitor the integrity of data and evaluate the accuracy of implemented IGA processes on demand, contributes to the maturity of an organization. The processes provide assurance to auditors and executive stakeholders that business rules and policies are being enforced. This enables organizations to demonstrate that they have applied the appropriate governance control and minimized the risk of non-compliance.

The auditing processes in IdentityPROCESS+ enables organizations to:

- Prepare audit-ready reporting on demand with a complete audit log, catalogue of compliance reports, in depth analysis, and manager dashboards
- Deliver a complete audit trail and history of changes to permissions, access requests, approvals and recertifications.
- Deliver fine-grained reporting on governance policies, enterprise roles, entitlements, and access data
- Generate and modify reports based on data, such as time periods, connected systems, and identities with graphical presentation of data for auditors / system administrators
- Facilitate auditors' and managers' assessment of the organization's compliance status at any given time

Actual versus expected state comparison

Automated auditing processes enable reporting and the evaluation of business policies and controls for the current actual state of identities and associated access rights, in comparison to the expected state. This enables the ability to alert administrators and system owners of any exceptions, such as invalid identity states or the creation of rogue accounts or permissions in managed systems. In addition, the auditing processes provide continuous compliance controls that support a timely and orderly remediation for policy violations.

The intention of establishing continuous compliance is to improve transparency through the operational controls. This makes it easier for auditors and executive stakeholders to rely on the IGA system to deliver business value. This results in the enforcement of compliance policies and the ability to maintain a complete audit trail of users' access rights across all on-premises and cloud-based systems.

SUMMARY

In this first part the IdentityPROCESS+ framework has been summarized to provide a business-level understanding of the different process areas of identity lifecycle management, access management, business alignment, governance, administration, auditing, and identity security breach.

The processes in each of these areas ensure that organizations can implement best practices to:

- Document who has access to what with a justification as to why
- On-board users with correct access rights, and terminate access when it is no longer needed
- Create or change access rights for employees and contractors as they change roles
- Improve efficiency when managing user identities through improved workflows and automation
- Perform ad hoc and periodic auditing, reviews, and analysis to ensure that users have the right access to the appropriate systems to do their jobs

Chapter 2
IGA Best Practices in Detail

Chapter 1 discussed how more and more businesses adopt hybrid IT environments on their digital transformation journey, to be effective and increase efficiency in a competitive market. However, unwanted challenges often emerge when managing identities and access across multiple applications, clouds, networks, and servers.

Typical challenges are:

- Lack of adequate security as organizations struggle to secure their on-premises and cloud-based applications to meet strict identity and access security requirements to avoid security breaches
- Non-compliance where organizations find it difficult to enforce identity and access governance policies and perform mandatory automated procedures to ensure they meet all internal and external regulations
- Maintaining efficiency as organizations struggle to ensure rapid implementation and secure onboarding of new digitized business processes, systems, and applications

An Identity Governance and Administration (IGA) solution solves these challenges, but like any other enterprise-scale deployment, a project like this requires a large variety of skills to achieve a successful implementation. Implementation of an IGA solution involves and impacts a great number of departments across the entire organization, requires technical integration with many other software products, and involves a wide variety of stakeholders – both inside and outside the company.

Organizations need to ensure they have all the skills in place to succeed as there are potential pitfalls that need to be addressed including involving the right stakeholders, the lack of available best practices, being overly ambitious, and underestimating the importance of data quality.

This is where the IdentityPROCESS+ best practices process framework comes in to play as it helps organizations avoid often seen pitfalls when implementing a successful IGA project. The framework provides best practices for each process from managing identity and access rights throughout an employee's career, ensuring good governance, managing user access in hybrid IT environments, aligning identity management with the business, to protecting critical digital assets before and after a potential breach has been identified.

In this chapter, the seven IdentityPROCESS+ areas; Identity Lifecycle Management, Access Management, Business Alignment, Identity Security Breach, Governance, Administration and Auditing, that were introduced in Chapter 1 are described in greater detail. When each of the processes within the process groups is implemented in an IGA system, they deliver functionality to address specific requirements ensuring adequate security, compliance with internal policies and external regulation, and maintaining efficiency when onboarding and governing identities and their access.

After reading this chapter, IT security professionals will have a full understanding of the different process areas as well as the individual processes that need to be in place to implement a comprehensive IGA system successfully.

NOTES ON THIS CHAPTER'S COMPOSITION

The IdentityPROCESS+ best practice framework is divided into seven IGA subject domains which are referred to as process areas.

Each process area is split into several process groups which contain a set of related processes defining specific IGA functionality.

Each process area description in this chapter is split into three sections:

1. An introduction describing how the process area addresses specific business requirements
2. Descriptions of the logical process groups and the processes they contain
3. Descriptions of how key stakeholders should be involved and the key best practices that should be considered when implementing the processes

While each of the process areas within IdentityPROCESS+ are interlinked, each section has been written to stand alone and therefore they do not have to be read sequentially.

Closing this chapter, a section describing how an organization should get started with an IGA implementation using the IdentityPROCESS+ framework is included. This explains which processes to focus on to get an essential overview of the organization's identities and their access, getting in control by creating the core identity and access data foundation.

TERMINOLOGY

There are many IGA-specific concepts introduced in this chapter. Rather than defining each when they are introduced which would disrupt the flow of the text, a glossary of key terms is provided at the end of the chapter.

Process Area

Identity Lifecycle Management

A key part of securing an organization's infrastructure is to ensure that user identities are properly created, changed, and disabled when employees join the company, move departments, get promoted, and leave the company. Identity lifecycle management processes enable the granting of access rights according to defined roles, rules and policies to ensure employees have the right access levels at any given point in time.

The task of ensuring the right user access may sound simple, but as illustrated in the figure below, this easily gets complex quickly. The figure shows the lifecycle of an individual who joined the company as a contractor, became an employee, moved to another department, got promoted, left on maternity leave, and eventually retired. At each stage of the person's employment, the job role requires access to different resources within the company.

Why identity lifecycle management is important:

1. To ensure employees always have the appropriate access they need to carry out their job efficiently
2. To enforce compliant access by ensuring employees do not have access to systems or data which they should not have
3. To enforce the principle of 'least-privilege' at any point in time
4. To limit the impact in case user accounts are compromised
5. To log and keep track of who approved what and for which reason

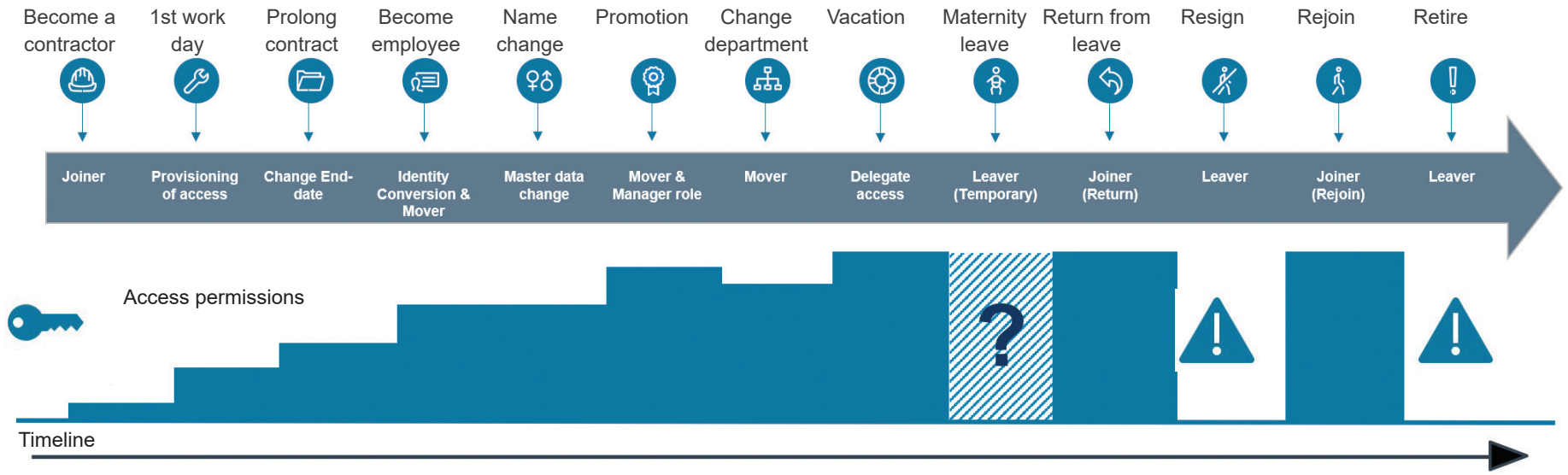


Fig. 2: An identity's access rights change during its lifecycle in an organization

Managing
The Identity Lifecycle

Identity Lifecycle Management processes include all the processes associated with the entire employment of an individual. Automated processes ensure that when joining a company, employees have access to all the systems, applications and file systems required to do their job, so they can be productive from day one.

As employees change job roles or get promoted, their access to existing systems may increase in line with the responsibilities of the new role. Likewise, a change to a different department, may require different access to systems or access to new systems. Finally, it may also be necessary, and is certainly a best practice, to remove any access to systems that the employee used in their previous job role, but is no longer required in the new role, so access rights do not accumulate over time. Failure to remove access systematically may result in violations of security regulations and compliance policies such as segregation of duty. This off-boarding of access rights is also handled by the Identity Lifecycle Management process area.

Extend security defenses

Handling on-boarding, changes, and off-boarding processes not only ensures that an employee can fulfill their job role, it also has the benefit that if a user account is compromised, an intruder will only have limited access to systems. The security boundary that these processes create is seen as adding further security to traditional security defenses such as firewalls and intrusion prevention systems and is referred to as the “identity perimeter”.

Identity lifecycle management not only focuses on employees as the actual environment is often more complex because companies typically also need to manage third parties such as contractors, seasonal workers, or business partners, who need access to company resources to work effectively with the company. If this complete lifecycle was to be managed manually, it would take a significant amount of IT resources to provision and de-provision individual accounts. Manual processing is also prone to human error which could leave the company exposed to unnecessary security and compliance risks. Instead, IdentityPROCESS+ automates the set of processes that manage all aspects of identity lifecycle management which are listed below.

The processes under the Identity Lifecycle Management process area are known as the joiner-mover-leaver processes. This is because the process area enables organizations to on-board, change, and off-board identities belonging to employees or contractors.

Common to all the processes, is that triggering any of them results in identities being updated in accordance with security levels, business policies, job role, organizational hierarchy, and context.

The full Identity Lifecycle Management process area includes the following process groups with subordinate processes:

Onboard identity (Process group)
- Onboard employee (subordinate process)
- Onboard contractor
- Onboard technical identity

Change identity
- Intra-organizational transfer process
- Master data change process

Off-board identity
- Termination

Process Group
Onboard Identity

Automates the creation of identities for employees and contractors when they join the company and allows technical identities to be created to manage business systems.

ONBOARD EMPLOYEE

The process ensures that the new employee is productive from day one with correct access to required systems for them to do their jobs.

Process description

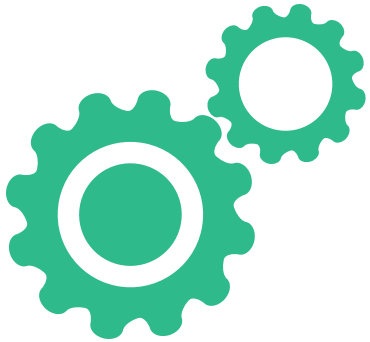
The onboard identity process generates a new identity automatically when a new employee record is created in the master HR system. The identity will be assigned pre-defined access rights which will not only give access to the resources that all employees are granted initially, such as Active Directory, email, relevant shared drives, and the company benefits system, but will also allow specialist applications, such as the purchasing application or developer tools, to be used based on role or context.

Best practice IGA system functionality

The new identity is made up of a unique user name and is imported and processed in the IGA system automatically. An approval task for the person in charge of the new identity such as the manager or administrator is created so they can confirm and approve the onboarding. The identity is set to inactive in the system until the 'Valid from Date'. The identity is automatically set to active when the Valid from Date is reached.

Technical process flow

1. When onboarding a new employee, HR creates an identity record in an authoritative source, for example a HR-management system
2. The identity record is automatically imported into the IGA system
3. The workflow steps are executed automatically
4. The IGA system reads the identity record and processes it according to predefined assignment policies



ONBOARD CONTRACTOR

Contractors and other temporary workers are an important part of business operations. Managing their identities has the same benefit as for fulltime employees - getting them working from day one with access to the right systems and resources.

Process description

The process is similar to the onboard employee process described previously. The manager responsible for the contractor creates a new identity and specifies which systems and resources the contractor should have access to. An important part of this process that is different than for managing permanent employees is to indicate the start and end date for the contractor to ensure that the identity only has access to relevant data during the contract period. Once approved, the contractor will have access to relevant data during their contract with the company.

Best practice IGA system functionality

The onboard contractor process is started manually by department managers when a new contractor is hired. The identity can also be created in the HR system if contractors are managed here. Otherwise, the identity can be created directly in the IGA system. The IGA system automatically detects if an identity with similar master data already exists due to a contractor having previously worked with the company. If a similar identity already exists, the manager is given the opportunity to either create a new identity or update the existing one. If start and end dates are specified, the IGA system automatically activates and terminates access on the appropriate dates. During the identity's active period, the contractor can request additional access rights directly in the IGA system which would be subject to approval by the manager.

Technical process flow

1. A user with suitable rights manually triggers the onboard contractor process by filling out an online form with the contractor's personal data
2. The user submits the form and the IGA system checks for conflicts or duplicates
3. If an identity with similar master data, such as name or email address, exists, the user has the option to create a new identity, update an existing identity, or terminate the process
4. The request is submitted for approval

! QUICK WIN...

The right access from day one:
If appropriate assignment policies are predefined, the new identity automatically gets access to basic access rights with minimal effort from IT, HR, and the hiring manager.

ONBOARD TECHNICAL IDENTITY

To eliminate the need to grant members of the IT team administrator access to systems from their personal identities, technical identities are used. As technical identities have privileged access rights and are used by several IT users, they need to be assigned an ultimate owner who is responsible for the governance of the account.

Process description

To ensure that these powerful technical identities are managed properly, the onboard technical identity process allows system owners to create the account and assign its responsibility to an actual user referred to as the primary identity. This assignment ensures that tight governance is maintained as the primary identity is responsible for the resource even though many other users may access the system and use the same account.

Best practice IGA system functionality

The system owner completes a technical request form in the IGA system which then creates the technical identity default properties. The technical identity is then mapped to an owner (the primary identity) who has the responsibility for the account. Once this mapping is complete, the technical identity is ready, and users can request access to use the technical identity to access the system for administration purposes.

Technical process flow

1. The system owner requests new technical identities for their systems using the request technical identity form
2. The technical identity is created, and the default properties are assigned
3. The technical identity is mapped to the owner (the primary identity)
4. The technical identity is ready for users to request access

! QUICK WIN...

Maintain tight governance:
Assign ownership of technical identities with privileged access rights to an actual user.

Process Group
Change Identity

Manages the access rights of employees and contractors as they change jobs or departments within a company and manages changes to employee personal data.

INTRA-ORGANIZATIONAL TRANSFER

When an employee or contractor moves within an organization, such as when they change department or are promoted, their user access rights need to be reviewed and updated to ensure the employee only has access to the appropriate systems. This safeguards against certain combinations of access rights that are prohibited by business policies, such as segregation of duties, being granted during the change.

Process description

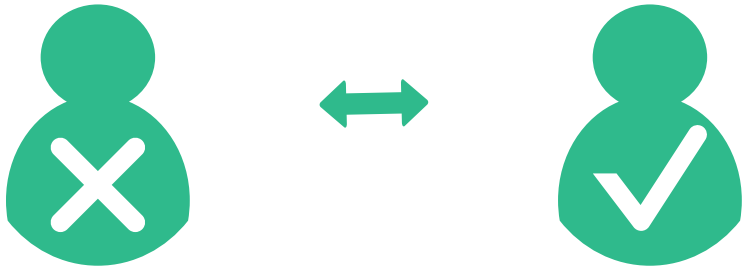
When an employee or contractor moves from one organizational unit to another or is promoted within their department, the intra-organizational transfer process revokes the access rights for the old role and adds assignments for their new role. Once this change occurs, it is approved by the individual's manager who can remove any direct resource assignments if necessary.

Best practice IGA system functionality

The process is initiated when an employee transfer or promotion is entered into the HR-system (the authoritative source). This event triggers the IGA system to clarify which new rules should be added or removed to an employee's account. Once this is complete, the account is ready for approval or further modification by the department manager. The manager has the option to add or remove access according to the job role. Access rights are automatically provisioned and de-provisioned in the systems. By default, removed access rights are maintained for a predefined number of days enabling the user to access and hand over work assignments.

Technical process flow

1. A job role change is entered in the HR-system / authoritative source
2. New access rights according to rules and policies for the new job role are automatically applied to the employee's account
3. The manager receives a notification to modify access rights to the employee's account
4. After manager approval new access rights are applied to the employee's account
5. After a pre-defined number of days, the user loses all access rights not recertified by the new manager



MASTER DATA CHANGE

Master data is stored in a central repository which is sourced from one or more systems. Gathering, updating, and managing master data across systems can be a difficult task. It is important to maintain good master data governance by ensuring that data changes are reviewed by managers and that changes are made in all systems.

Process description

The master data change process streamlines the requested changes, updates, and additions to an organization's master data and ensures that the change is copied to systems connected to the IGA system.

Best practice IGA system functionality

Users can change their data records through a data update request, which must be approved by the identity's manager. When the IGA system detects a change in master data records, the change process is initiated to gather the modified data and update it in the IGA solution according to predefined data-mapping rules. Any modification to an identity's master data is then automatically propagated to connected systems based on previously defined provisioning rules.

Technical process flow

1. An employee makes changes to his/her personal data
2. The change triggers an event to the manager who is responsible for the specific employee's data change
3. The manager rejects or approves the change request before it is executed in systems and sub-systems

! QUICK WIN...

Master data governance:
Ensure data changes are reviewed and that changes are carried out across all systems.

Process Group
Off-Board Identity

Manages the off-boarding of employees when they resign or are dismissed so that they no longer have access to business systems once they leave the company.

TERMINATION

Organizations need to ensure that employees and contractors do not have access to systems after they have left the company on a temporarily or permanent basis.

Process description

The termination process covers both the immediate off-boarding of an employee or contractor, as well as planned permanent off-boarding which is implemented when a user has resigned and needs access to systems during their notice period. The process automates the terminating of access rights or disables applications in the systems ensuring these are properly de-provisioned and the user cannot access data after they have left the organization.

Best practice IGA system functionality

The process is triggered when:

- The valid to date in the identity record of the HR system or your IGA solution has been reached. That happens for example to contractors who have pre-defined end-dates
- The identity record is no longer delivered by the source system. This happens if the data record is deleted after an employee has left the company

In either scenario, and when the process is voluntarily or involuntarily triggered, the identity is terminated, all its accounts are disabled, and access revoked.

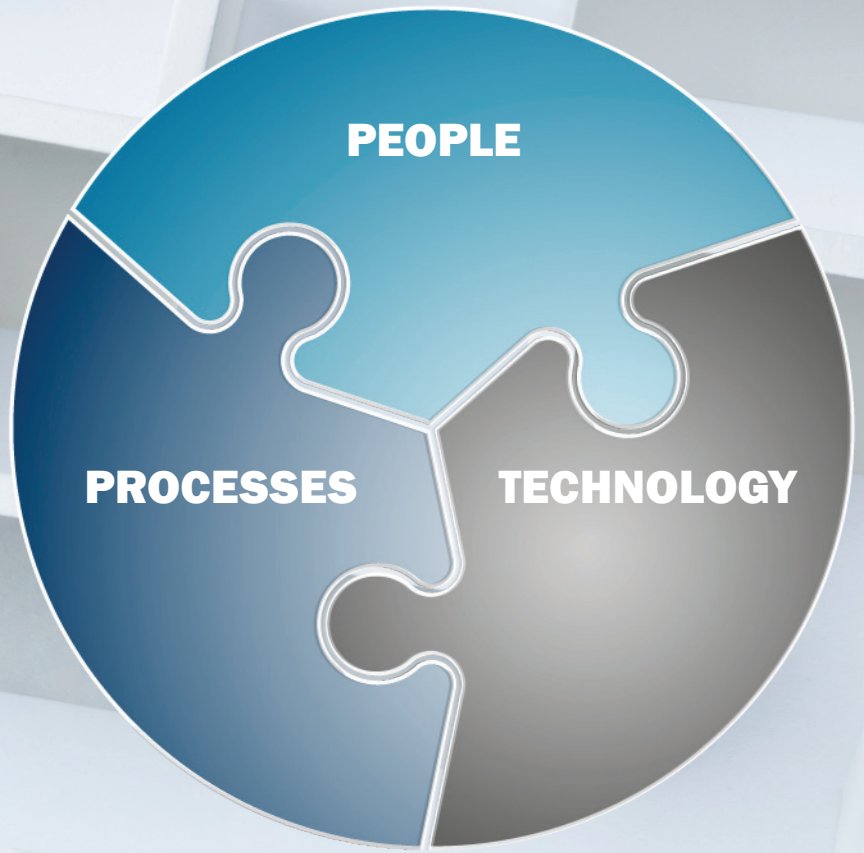
Once an account is deleted, the transfer ownership process begins to start moving the responsibility for resources owned by the deleted account to other users.

Technical process flow

1. The valid to date or value in the identity record of the HR system or the IGA solution is reached, or a missing data set triggers the process in the IGA solution
2. Identity status is set to Terminated
3. The identity is terminated, all associated accounts are disabled, and access is revoked
4. The transfer ownership process is triggered by the IGA system to ensure that all resources previously owned by the terminated identity are re-allocated

Implementing Best Practice
Identity Lifecycle Management

The successful outcome of implementing Identity Lifecycle Management requires involvement from appropriate stakeholders and a thorough pre-analysis to define data, rules, and policies, so processes can be customized according to the organizational structure.



PROCESS STAKEHOLDERS

As the definition and implementation of the identity lifecycle management process involves many different departments, it is important to ensure that the relevant stakeholders are included and informed of their duties early in the project. Communication of these expectations will ensure that all parts of the process are covered which will result in the smooth implementation of the identity lifecycle management processes. The table below shows a list of the key stakeholders in the Identity Lifecycle Management process area along with their involvement, responsibilities and tasks they are expected to perform pre- and post-implementation.

Stakeholder	Involvement	Why are they involved?	Pre-implementation tasks	Post-implementation tasks
Human resources (HR)	HR is involved at the start of the project and is continuously involved throughout the entire IGA project. HR's work touches all aspects of identity lifecycle management as HR data is key to the operation of all processes.	HR is initially involved to ensure the integrity of the data in the HR system (the authoritative source) as this data is used to assign roles and therefore access rights to individuals. Post-installation, they are involved in making changes to employee records which are used by the IGA system to provision and deprovision access.	1) Ensure that employee records are clean and consistent. 2) Give the IGA team the necessary access so they can import data from the authoritative source into the IGA system.	1) Create new employee records accurately in the HR system so the IGA system can accurately grant access rights. 2) Make changes to employee records to reflect their status (e.g. current job role, manager). 3) Ensure consistency in data input to maintain data integrity so the IGA processes can run properly.
IGA team	The IGA team starts working with HR early in an IGA project as they must ensure the data integrity in the authoritative source (the HR system) before it is uploaded into the IGA system. The IGA team has no direct involvement in the identity lifecycle management processes.	The IGA team needs to verify the integrity of the employee data imported into the IGA system as this forms the basis for many processes. Without data integrity, the processes in the Identity Lifecycle Management process area would be unreliable due to processes being run using inaccurate data.	1) Work with HR to ensure clean employee records. 2) Integrate the HR system and other potential authoritative sources into the IGA system.	Monitor data import integrity.

Stakeholder	Involvement	Why are they involved?	Pre-implementation tasks	Post-implementation tasks
Line managers	Line managers' involvement starts once the HR data has been loaded into the IGA system. Regarding identity lifecycle management, they are involved in approving onboarding of employees, contractors, intra-organizational transfers, master data changes, and termination of user identities.	As line managers are most qualified to know how their department operates, they are in the best position to define roles and to grant/revoke user access requests, as well as to approve master data changes.	Work with the IGA team and Business System Owners to define roles based on their knowledge of the employees in their department.	Approve employee onboarding, contractor onboarding, intra-organizational transfers, master data changes, and termination of user identities.
End users (employees and contractors)	Once the IGA system has been implemented, end users can be involved in any of the identity lifecycle management processes. In some cases (onboard employee, onboard contractor, intra-organizational transfer, and termination), they are indirectly involved as their manager interacts with a process on their behalf while in others (master data change), they interact with the process directly.	The processes in the Identity Lifecycle Management process area involve end users when they join-move-leave the company or when they need to make changes to their personal data.	None	Make changes to master personal data where appropriate.
Business system owners	Once the HR data has been loaded into the IGA system, business system owners start working with the IGA team to onboard business systems into the IGA system. Regarding entity lifecycle management, Business System Owners create technical identities for the systems they are responsible for using the onboard technical identity process.	Business systems owners are involved in the identity lifecycle management processes because they are responsible for the security and governance of their systems. Therefore, it is their responsibility to create technical identities so IT administrators can access and manage their systems.	None	Create technical identities so IT administrators can access and manage their systems.

Key Best Practice Recommendations

Below are a set of key best practice recommendations that should be taken into consideration when implementing the identity lifecycle management processes in IdentityPROCESS+.

DATA MANAGEMENT

Define data quality

As employee and contractor data is critical to the success of an IGA project, rules governing data quality must be defined. This includes identifying the interfaces to the business systems and how the data transfers between them and the IGA system are to be optimized for quality.

Determine the master data sources for personnel records

Every IGA system relies on personnel records to implement the processes in the IdentityPROCESS+ framework such as assigning access rights to an identified role or routing access requests to an employee's manager for approval. To ensure that these processes run effectively, it is important that the right data is imported into the IGA system.

However, this situation may be complicated due to there being many different sources of personnel records. The data required could be:

1. Stored in multiple, independent systems across the organization, or
2. Duplicated across different systems in the network

If employee data is held in multiple, independent systems then connectors need to be used to transfer data between each system with the IGA system. However, if data is duplicated - either because some is held in the HR system with some being stored within Active Directory, or because a redundant system has been set up to improve system performance - then the organization needs to decide which source should provide the master data for attributes. This decision then needs to be implemented in the IGA system, so that each piece of information comes from one defined source. For complex environments, this could result in a lot of logic being required.

This decision is one of the first considerations for an organization looking to deploy an IGA solution as without clean data, the IGA system cannot function properly. In addition, as the sources of employee and contractor data can be very complex, the definitions of the master data sources need to be done by the organization itself as this cannot be carried out solely by an IGA vendor or third-party integrator. However, IGA vendors will work with the organization to ensure that the data meets the necessary requirements.

Load master data before implementing processes

All the master data should be loaded into the IGA system before work is started on implementing any processes. If this is not done, processes like recertification will have to be carried out after each data load which wastes time and resources.

Determine the frequency of data imports from authoritative sources

HR system data changes frequently due to employees joining the company, getting promoted, or leaving. As a result, data needs to be regularly imported from the HR database (or other authoritative source) into the IGA system. The import frequency depends on business requirements. Typically, once per day is adequate for most organizations. However, for organizations where employees need to be onboarded the same day, it may be necessary to import data every two to four hours.

IDENTITIES

Ensure that rules are in place to create unique identities
It is critical that all identities in the IGA system are unique. If no identity naming policy is in place, then it is necessary to create one. Also, it is a good idea to have the naming policy explicitly written down for the entire organization.

Do not tie user IDs to identity data
This ensures a seamless change in the event of, for example, a user changing their name as there is no need to change the actual identity.

Do not reuse user IDs for returning employees or contractors
If an individual leaves the company and rejoins later, it is recommended that a different user ID is created regardless of whether it is an employee or contractor. By doing so, the organization can be confident that there is a separation in logs and historical records showing the requests and changes of access rights. The new user ID makes it easier to analyze the different employment periods during company audits.

GOVERNANCE AND STANDARDS

Consider optimizing business processes to reduce complexity
The current business processes, if any, need to be assessed. If they are not fixed due to a regulatory framework that must be adhered to, it is recommended that the organization consider the possibilities of refreshing outdated processes and reducing any complexity. It should be noted that if there are different processes across the organization, such as one process for bank traders not being the same as for other employees, standardization will be difficult. In these cases, process optimization must be considered.

Review processes
The implementation of an IGA solution is a good time to review processes across the organization to ensure that they are all appropriate to support the business going forward. It is often possible to significantly reduce complexity and increase overall efficiency by removing outdated processes as well as automating others. An example of this might be that in the past, managers had to request access to systems on behalf of their direct reports as this was the only way to work in their old IGA system. With the introduction of self-service capabilities, employees can request their own access to business systems which reduces the manager's workload.

Ensure documented standards are compliant with current and expected future legislation requirements
Having documented standards is important from a compliance perspective and helps prove to auditors that the organization understands regulatory requirements. As part of the analysis of the existing standards in the organization, it is recommended to include analysis of future compliance requirements to prevent additional work whenever new legislation comes into force.

Identity Lifecycle Management Questions to consider

- What are the sources of your master data?
- How is the master data to be delivered?
- Are there rules in place to create unique identifiers?
- Are there governance procedures in place to run processes?
- Are the current standards documented and compliant with current and future legislation requirements?

BUSINESS RECOMMENDATIONS

Involving business managers early in the project

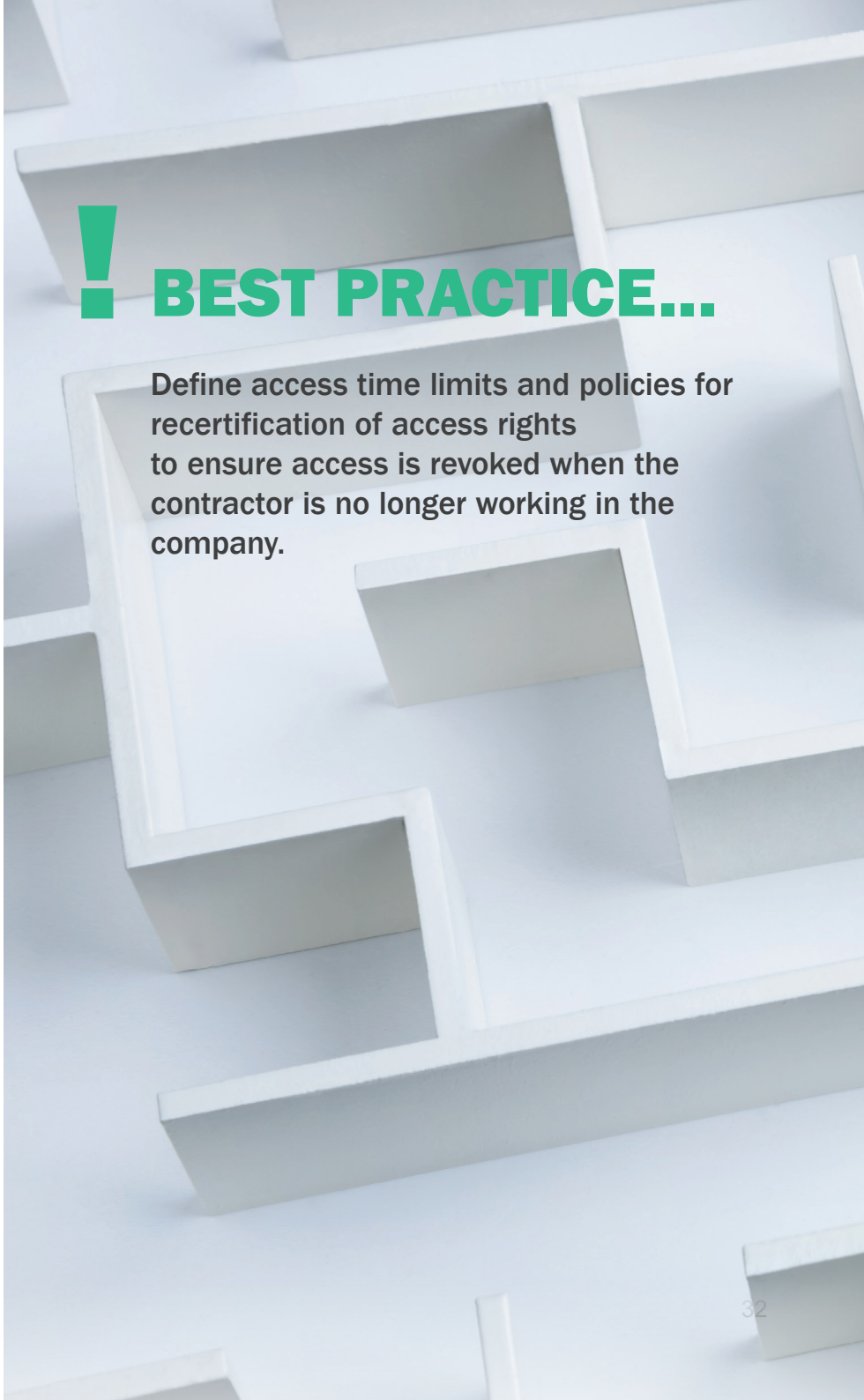
Many decisions associated with defining the parameters for identity lifecycle management need input from individuals who understand the business requirements. These requirements could include legal and compliance needs to ensure, for example, that data is kept for a given period, as well as individual requirements for different countries and industries. It is therefore recommended that stakeholders from across the organization are brought into an IGA project early so that business requirements can be built into the processes at an early stage instead of trying to retrofit them after the deployment.

Manage contractors to ensure compliance

To ensure good governance, organizations should ensure that a legal contract is completed before onboarding a contractor into the IGA system. Having a contract in place helps ensure that the contractor will abide by the rules and regulations of the company and will satisfy audit requirements. It is also recommended that access rights for contractors are limited to a finite time such as 3 or 6 months. This is particularly relevant if the organization is governed by strict regulations. Failure to do so could result in user access being forgotten and an ex-contractor having access to business systems long after they have left. Time limitations of how long access should be valid must be defined – preferably by HR.

Maintain a written IGA policy

Many areas of running the identity lifecycle management processes involve making decisions that are outside of the IGA system. These include determining how long contractors should be granted access to business systems before their access needs to be recertified, the use of non-personal technical identities, and grace periods when access is transferred from one employee to another. To prevent ad hoc decisions on policy from being made which could result in governance violations, it is recommended that a formal written policy is put in place. Without a written policy, the granting of access could become non-compliant, there will be a lack of consistency across different divisions, or significant amounts of time will be wasted on discussions for each individual case.



! BEST PRACTICE...

Define access time limits and policies for recertification of access rights to ensure access is revoked when the contractor is no longer working in the company.

Summary

Identity lifecycle management encompasses all the processes of an identity lifecycle from starting as an employee or contractor all the way through to termination of employment. This includes all the steps throughout the employee's work life including name changes, temporary maternity leaves, leaving and rejoining the organization, and more.

In an adaptable identity lifecycle management solution, business functions can be matched according to changing business needs. This includes processes for IT and business collaboration, segregation of duties (SoD), and industry specific role and policy models allowing any arbitrary levels of roles, role types, and classifications.

Modern lifecycle management models integrate multiple applications and systems (some identity parts managed within an application like ERP and some in identity stores like Microsoft AD) into logical business applications management for easy application and system resource onboarding, self-service access request, and governance reporting.

Process Area
Access Management

The access management processes defined in IdentityPROCESS+ allow organizations to control the granting of access rights while ensuring that they do not violate any security and compliance policies such as segregation of duties.

When identities have been created by the identity lifecycle management processes new employees or employees moving around the organization will have the access rights they need to perform their day-to-day job duties. Over time, employees may need to extend access rights to a system because they have been assigned to a new department or region, or because they get promoted and require access to additional functionality in applications they already use. Similarly, new applications may be introduced as the business develops that employees need to request access to use.

Traditionally, IT departments used to keep track of access rights in spreadsheets to document their process to auditors. The problem with this traditional way of handling the process is that it is very time-consuming, prone to errors, and may violate internal policies or external regulations. Documentation used for audits may be fragmented as reasons for granting access are not properly logged and employees may accumulate access over time because they are not revoked when they move department or stop working on a project.

The access management processes defined in IdentityPROCESS+ allow organizations to control the granting of access rights while ensuring that they do not violate any security and compliance policies such as segregation of duties. Also, the definition of self-service access requests means that the processes reduce the amount of work required by the IT department as processes associated with granting access are automated and delegated. The processes also describe how to set end-dates to ensure access is removed when it is no longer required by the user.

Why access management is important:

1. Allows users to request additional access to business applications
2. Gives managers and systems owners the ability to approve or deny access
3. Ensures existing access can be transferred to another user if necessary

Access management consists of three process groups including request access rights, which simply describes how users can request access, evaluate and act - which includes processes for approval and removal of access as well as delegation of access rights, and finally the provisioning group that looks at how to grant access to less-used systems that are not connected to the IGA system.

The process groups in the process area 'Access Management'

Request access rights
- Access request

Evaluate and approve
- Approval of access requests
- Delegate access
- Remove access

Provisioning
- Manual provisioning

Process Group
Request Access Rights

Automates access requests enabling end users to provide the right information so that access can be granted quickly without introducing security and compliance violations.

ACCESS REQUESTS

Over time, users need to request more access to systems as they progress through their employment. It is important that they are granted the right level of access and the reasons for access are properly documented for auditing purposes.

Process Description

When the request access process is initiated, the user is prompted to fill in the business justification for the new access rights. The process then triggers the approval of access request process during which the manager will either approve or reject the request. If approved, the access is automatically provisioned, and the user will have the new access. Requests can be made on behalf of other people so that a manager can request access for a contractor or employee who is not as familiar with the system.

Best practice IGA system functionality

The user makes the access request directly in the IGA system and can only submit the request once a business justification, as well as information on business context (department, project, or cost center), is provided. Upon submission, the access request approval process is initiated. A segregation of duty policy check is executed automatically to ensure that the new access will not grant a toxic combination of access for the user. An approval log is created for each requested resource task, enabling approvers to see the identity and the reasoning for the approval.

An approval history is maintained for each requested resource assignment. The history is accessible to the approvers in the process and enables them to see who previously approved the request when and why.

Technical process flow

1. The user logs in and begins the access request workflow by filling in details of the request such as: Identity that the request is for, the reason for the request and the business context
2. The user requests for its own identity or for other managed or owned identities. Optionally, the user can specify a user account for which the resource is requested for, as well as specify a validity period for the requested access
3. The user searches for roles and resources to request, and if resources require the user to select or specify an attribute, these are selected.

Fig. 3: Steps in the access request process

Process Group
Evaluate and Act

Manages the routing of self-service access requests for approval, automates removal of access rights that are no longer needed, and processes the delegation of access rights to cover an employee leaving or an extended absence.

APPROVAL OF ACCESS REQUESTS

Before a user access request can be granted, it needs to be checked to ensure that it is not in violation of conflict policies such as segregation of duty, and then approved or rejected by the business system owner.

Process description

The approval of access requests process is closely linked to the request access process and starts when a user has requested access.

The process includes four tasks:

1. The request is received by the designated approver, typically the business system owner or manager, who can grant or reject access after reviewing the request
2. A segregation of duty (SoD) policy check is carried out to ensure that granting the request does not give the user access to carry out activities which contravene company policies
3. A log showing the history of what has been approved, when, and why is maintained. This log helps the approver assess the suitability of access requests in the context of what has been granted or rejected previously and documents the process for auditing purposes
4. Access is granted if the request is approved and does not violate any predefined business policies

Best practice IGA system functionality

Once the request access process is executed, the IGA system automatically creates a task for the relevant approver. An SoD policy check and other configured conflict process checks are executed and the information log is updated with relevant information. The IGA system determines what needs to be provisioned to satisfy the request and sends this information for provisioning.
An approval history is maintained for each requested resource assignment. The history is accessible to the approvers in the process and enables them to see who previously approved the request when and why.

Technical process flow

1. The incoming access request is either approved or rejected
2. Role and policy calculations are triggered including SoD violations evaluation
3. Provisioning to target systems is executed

DELEGATE ACCESS

Occasionally, it may be necessary for a user to assign his/her system access rights to a colleague, for example during holiday periods. A manager may want to delegate their access rights to a personal assistant or project coordinator for a longer period. This type of access delegation is temporary and therefore the overall access rights remain with the delegator to ensure ongoing compliance.

Process description

The delegate access process allows users to temporarily assign their access to other users. The process contains several procedures ensuring that the transfers do not leave an organization open to unnecessary security risk.

One of the procedures ensures that if the delegated access rights are withdrawn from the delegator, then they are also immediately removed from the employee they have been delegated to. Another ensures segregation of duty (SoD) policies are checked for toxic combinations during the delegate access process. Finally, it is possible and best practice to limit the delegation to a defined period such as the length of time the delegator is on holiday or the estimated time they will be on leave. This ensures that the increased access level is not forgotten, so a user will not accumulate excessive access over time.

Best practice IGA system functionality

To execute the delegate access process in the IGA system, the delegator chooses the access rights they want to delegate, the user they want to delegate access to, and the validity period. The system automatically assesses if any policies are violated and either rejects the request or provisions the access.

Technical process flow

1. The user chooses an identity that they want to delegate the access rights to
2. The user chooses the access rights to be delegated and fills the Valid from and Valid to fields
3. The user submits the request
4. Roles and policies are calculated for the identity
5. The delegated access rights are provisioned

REMOVE ACCESS

To maintain a high level of compliance and security, organizations need to remove user access that is no longer needed when employees or contractors leave, move to a different department, or get promoted.

Process description

The remove access process ensures that access rights are removed when they are no longer needed and is triggered when:

1. An identity removes its own direct access
2. A manager removes direct access for one of their direct reports
3. A system or resource owner removes direct access to a system or resource he / she manages
4. A previously granted access right meets a preset expiry date
5. A data administrator can always determine to remove direct access of any identity

Best practice IGA system functionality

A user or manager logs into the IGA system and selects the access to be removed. Once selected and confirmed the access is removed and deprovisioned in the target system. If the process is triggered by an expiry date the same steps are executed automatically.

Technical process flow

1. The user logs in to the IGA solution and opens the overview for the identity that he/she wants to remove access to
2. The user selects the desired access and confirms
3. Access is deprovisioned

Process Group
Provisioning

Manages the recording and logging of access rights provisioning for business systems that cannot be automated in the IGA system.

MANUAL PROVISIONING

While it may not be possible or desirable to connect all business systems in an organization to the IGA system, it is still necessary to enable access and log activities for compliance purposes.

Process description

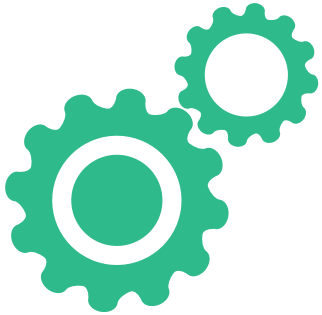
One of the key benefits of an IGA system is that the process of provisioning or assigning access rights for a user in the target business system is automated. The manual provisioning process ensures that you can provision to systems not connected to the IGA system and still monitor and log activities within the IGA solution to meet auditing and compliance requirements. The request is done in the IGA system and the provisioner, the user or user group responsible for handling the request, gets a notification to carry out the task which is done manually. Both the requester and provisioner logs relevant information in the IGA system.

Best practice IGA system functionality

The requester makes the request directly in the IGA system and the provisioner is sent a manual provisioning task. The provisioner manually performs the actions required to create the assignment between the identity and the resource in the target system and confirms in the IGA system that the task is completed.

Technical process flow

1. The IGA system determines that an access assignment requires manual provisioning as it does not have an actual desired state
2. The IGA system creates a manual provision task
3. An e-mail notification is sent to each person responsible for the manual provisioning who will access the target system and provision access manually
4. The manual provisioning is confirmed in the IGA solution by the provisioner
5. The IGA system updates the actual provisioning claim as being unconfirmed (i.e. the system has not confirmed the actual state itself)



Implementing Best Practice
Access Management

The successful operation of the access management processes relies on a combination of the end users being able to request new access rights and their line managers efficiently approving or rejecting those requests.

PROCESS STAKEHOLDERS

The access management processes are mainly end-user focused. This means that the tasks associated with these processes are all post-implementation and only involve end users and their line managers. HR, the IGA team, and business system owners have no direct involvement in these processes.

Stakeholder	Involvement	Why are they involved?	Pre-implementation tasks	Post-implementation tasks
IGA Team	None	None	None	Monitor process flow. Exception handling when approvers are not available.
Line Managers	Line managers respond to the request access process by either approving or rejecting the request. Line managers can also remove access from one of their direct reports if necessary.	Managers are usually in the best position to approve, reject, and remove access rights from their direct reports as they understand the business situation and the use of the associated business systems.	None	1) Analyze access requests when an action is assigned to the line manager and approve or reject based on the information available. 2) Remove access from direct reports when they no longer need access to the particular business systems.
End Users	End users request new access rights if they feel they need to access new business systems to carry out their work. End users may also select to delegate their access rights if they are to be out of the office for a period.	End users need the capability to request access to new systems and to delegate existing access rights.	None	1) Use the request access process when they need to access new business systems. 2) Use the delegate access process when they want to give their access rights to another user on a temporary basis.
Business System Owners	Business system owners need to approve access requests.	Business system owners are responsible for the security of their systems and therefore need to approve access rights for users.	None	Respond to access rights on an ongoing basis.

Key Best Practice Recommendations

Below are a set of key best practice recommendations that should be taken into consideration when implementing the access management processes in IdentityPROCESS+.

ACCESS RIGHTS

Determine if some users can request access rights for others

It may be appropriate for certain users to request access rights on behalf of other employees. For example, an organization may allow managers to request access to business systems for their direct reports, or personal assistants may need to request access for their managers.

Allowing some users to request access on behalf of others will help increase overall efficiency and speed up operations, but measures need to be put in place to minimize misuse. The circumstances where individuals are permitted to request access for others should be documented in a written IGA policy document.

Determine who can remove access rights from individuals

The removal of access rights could result in preventing an employee from performing their day-to-day job function. However, there may be certain times where access rights need to be removed such as when a security breach is suspected, where there is a segregation of duty violation, or where the organization suspects that the user is in violation of its information technology usage policy.

Organizations need to ensure that employees with the ability to remove access rights understand the business implications of doing so. The circumstances where individuals are permitted to remove access should be documented in a written IGA policy document.

APPROVALS

Determine if an approver can modify requests

It may be appropriate for an approver to be allowed to modify a request. For example, if the approver feels that the 'valid to' date does not meet with compliance guidelines. Allowing changes to be made will speed up the approval process but needs to be managed carefully to ensure that changes are in line with organizational guidelines. If changes are permitted, the process should be explained in a written IGA policy document.

Determine whether an implicit or explicit model for granting user access should be adopted

To improve efficiency, some organizations give a certain level of access rights - often referred to as birth rights - to users based on a set of predefined rules. However, other organizations that are more risk averse enforce an explicit approval step in each case.

Both options have their merits but also their drawbacks – organizations need to determine which is most appropriate to meet their needs. Implicit granting of access is efficient because it does not need a manager to approve basic access rights that all new employees will be granted based on their basic job role requirements (e.g. e-mail, Active Directory, and expenses application). However, to implicitly grant access, role definitions need to be in place.

For explicit approval, there are fewer upfront steps needed as no roles need to be defined ahead of time, however, access rights need to be approved for each new employee.

It is recommended that, where possible, organizations should use predefined rules to assign access rights as this reduces the workload of the approving managers and reduces the time taken to grant access rights to users.

Use line managers for access rights approvals

It is important that line managers know what access their direct reports have been granted. For this reason, it is recommended that all approval processes are routed through line managers. If appropriate, approvals could also be required by data or application owners, but this should only be considered for sensitive applications as it will add additional steps which will slow down the approval process.

COMPLIANCE

Enforce validity periods for external users

To improve compliance, external users such as contractors and third-party business partners should only be granted access for a limited period such as three or six months depending on the sensitivity of the resource, they are being granted access to and the level of access required. While this introduces an extra task for the approving manager on a regular basis, it also introduces a level of compliance which ensures that short-term workers are not left with access after they leave the company.

Increase compliance using resource classification

To increase efficiency when managing compliance requirements, it is recommended that resources are classified using tags. Classifying different resources based on the type of data they process, makes it easier to establish how they need to be managed and therefore which access policies need to be enforced based on regulatory requirements such as GDPR.

MISCELLANEOUS

Ensure that business continuity is taken into consideration

Organizations need to identify if there are business critical applications that the company depends on where granting only one individual access rights could result in problems with business continuity. For example, an organization would face challenges if the only employee who has access to the server backup software is out of the office when data needs to be restored.

Use notifications sparingly

As managers are often overwhelmed with e-mail notifications, they are likely to overlook and miss important updates. It is recommended that organizations consider whether users need to be notified about every event in the IGA system. Instead, organizations should consider requesting that line managers log into the IGA system and process their task lists on a regular basis which ensures that they will not miss any important actions they need to perform.

?

Access Management
Questions to consider

- Who can request access rights on behalf of other users?
- Who is permitted to remove access rights?
- Should an approver be able to modify an access request?
- Should access rights be granted implicitly or should explicit approval be needed?
- Are there any access rights that are needed to ensure business continuity?

Summary

Access management contains all of the processes to manage user requests starting with a user requesting access to a system which is then approved by managers or business system owners through to the removal of access when it is no longer needed by the employee.

Access management also allows for the delegation of access rights to other employees either on a short-term or long-term basis.

A mature IGA solution allows users to request access to the business systems or applications they require, automatically routes the request to relevant approvers and performs checks to ensure that any granted access does not violate segregation of duty or other policies.

Process Area
Business Alignment

Once fully implemented, an IGA system will be handling all identities associated with an organization. For some organizations, this may be thousands of identities made up of employees, technical identities, contractors, devices, and end-users.

If all of these identities were to be handled on an individual case-by-case basis, the job would be very time consuming and extremely complex. Just imagine how complex the monthly onboarding of for instance 10 new employees across the organization would be. They would be joining different departments and some could belong to multiple teams and multiple projects. However, as many employees require the same or similar access rights to perform their day-to-day work, granting of access can be significantly simplified by grouping employees together based on what they do (roles) and where they work (context).

Why business alignment is important:

1. To simplify IGA processes for non-technical users
2. To make the maintaining of access for employees with the same job role or business situation efficient
3. To effectively manage fine-grained definitions of access constraints

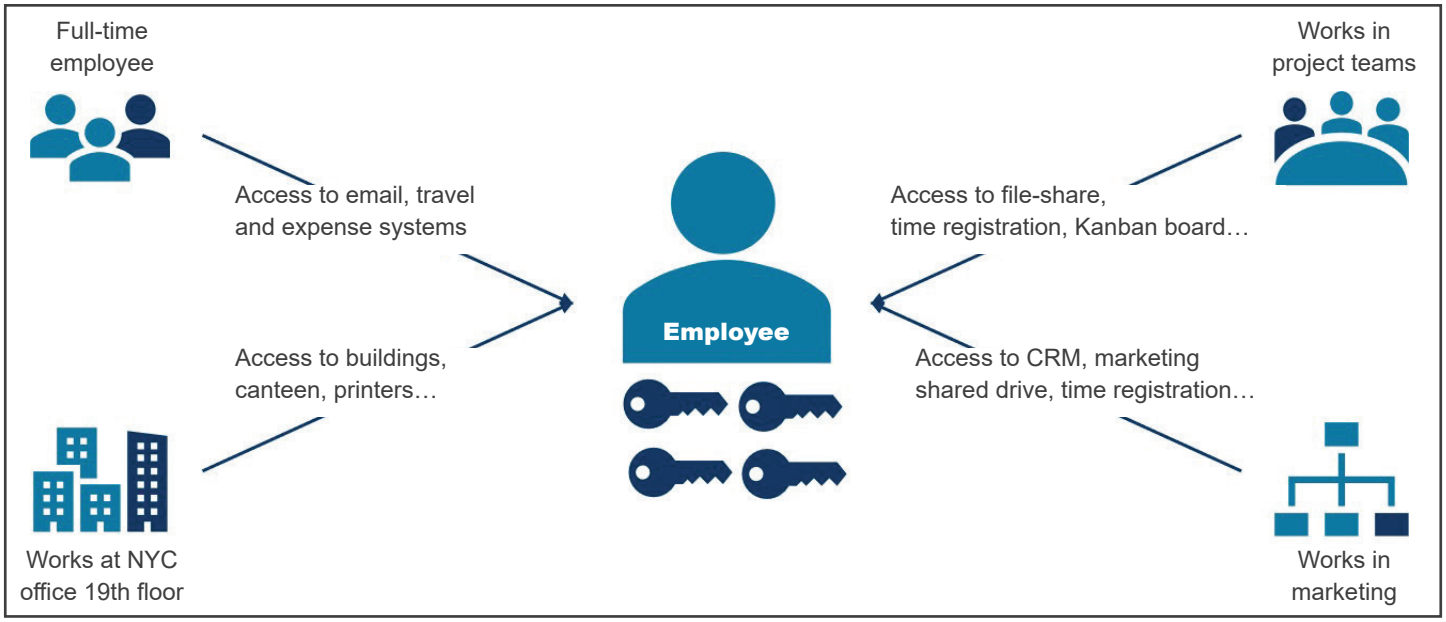


Fig. 5: Creating roles, contexts, and policies aligned to the business simplifies your identity and access governance.

Managing
Business Alignment

The business alignment process area reduces the complexity of onboarding and managing employee access rights using roles, policies, and contexts with predefined access rights to which employees can be assigned. The defined policies and contexts can be designed to accurately model and reflect the business structure in the IGA solution.

Overall, this allows organizations to optimize their IGA deployment and achieve quick wins early in the lifecycle of the project due to increased user adoption. The three process groups are further explained below.

Manage roles

Business Alignment starts with the definition of roles which are lists of access requirements for users who have the same or very similar jobs. If there are multiple employees in an organization that have the same role - such as sales managers and helpdesk support agents - defining roles makes it easier to get them up and running when they join the company.

Manage policies

The business alignment processes enable assignment policies to be defined which automatically assign a set of rights to individuals if they meet certain criteria. For example, this could be access to a file share for all people in a certain department, or for access to printers for all employees located on the third floor.

Assignment policies can be set with a specific start and end date to limit access which will keep the company secure and compliant.

Manage context

Like roles, contexts make managing groups of users with similar access requirements easier as they can be treated as a single entity. However, they are different to roles because the individuals being managed do not necessarily have the same job function but have a common business interest. For example, a group of employees working in a manufacturing production line may all need access to the same production database even though they perform different roles. In this case, the different job functions would all be part of the “manufacturing plant workers” context.

Contexts allow companies to model and govern complex situations such as matrix management structures or organizations where employees are associated with multiple departments.

The Business Alignment process area includes the following process groups and sub-processes:

Manage role

- Create, modify, or terminate role

Manage policy

- Create, modify, or terminate assignment policies
- Create, modify, or terminate constraint policies

Management context

- Create, modify, terminate, request and approve, prolong, and remove context assignments

Process Group
Manage Role

Enables organizations to quickly and easily assign a set of access rights to new users with the same job roles.

CREATE, MODIFY, OR TERMINATE ROLES

Assigning access rights to users manually is time-consuming, tedious and prone to human error. By creating a set of access rights (a “role”) for a common job function and using it many times, organizations increase efficiency and reduce the likelihood of mistakes that result in security and compliance risk.

Process description

The manage role processes which include create role, modify role, and terminate role allow administrators to manage descriptions of access requirements for users who have the same or very similar jobs. When a new employee joins the company and is assigned a role, access is automatically provisioned to all the systems they need to perform their job. For example, all sales personnel should be granted access to the company’s CRM system, e-mail system, expense, and travel application, so instead of being granted the access individually they are all granted when a new sales employee joins the organization.

In addition, roles can be modified over time to match new business requirements such as new applications being introduced for a certain job and can also be terminated when they are no longer required.

Best practice IGA system functionality

Access requirements that are required to meet business needs for each job function are defined using the create new roles process. Roles are defined to match organization structures, business locations, business processes, or control procedures. They are defined in conjunction with relevant legislation, regulatory demands, and company security policies. Once defined, the roles are created in the IGA system and assigned to new employees based on their job description in the HR system when they join the company or when they move to a new job function.

If there is a change in the business need represented by the role, such as a new application being introduced or a new regulation, then the modify roles process is used to update role definitions. When the business need is no longer relevant, the terminate roles process is used to remove a role from the IGA system.

.

Technical process flow

1. The administrator creates roles based on attributes such as job titles
2. The IGA system determines whether each identity matches the role
3. Associated access rights will be provisioned to identities matched up to the specific role

Process Group
Manage Policy

Enables organizations to quickly and easily assign a set of access rights to users who meet a set of criteria and to create and manage access constraint policies.

CREATE, MODIFY, OR TERMINATE ASSIGNMENT POLICY

Setting up individual access rights for users that meet certain criteria - such as users in a department who need access to confidential data - is inefficient and potentially error-prone. Establishing procedures to automate assignments based on policies not only improves efficiency, but also decreases the security and compliance risks due to incorrect access rights assignments.

Process description

The assignment policy processes which include create assignment policy, modify assignment policy, and terminate assignment policy, manage the policies giving access rights to users matching certain business criteria that results in them needing access to business systems and data.

Unlike roles, which use the employees' job titles to assign access rights, assignment policies depend on matching identity characteristics. Any identity that falls into the identity filter set in the assignment policy will be granted the associated access rights. For example, a manager based in the US would be granted access to the company's US-based expense management system whereas their European counterpart would be granted access to the equivalent European system.

Best practice IGA system functionality

The administrator sets up an identity filter and creates a new assignment policy using the create new assignment policy process. Any identities that match the filter criteria are automatically given the access rights defined in the assignment policy. Any changes in the business requirements can be reflected using the modify assignment policy process.

If an assignment policy is removed using the terminate assignment policy process, then any access rights that were set up by it will be removed. It is important that the consequences of the terminate assignment policy process are considered before it is used as end users may be left without access to applications that are critical for them to do their job.

Technical process flow

1. The administrator creates the assignment policy which includes when the policy is valid as well as the filter defining the identities, contexts, and account types that should be included. The assignment policy also includes a list of resources that should be allocated to identities matching the filter
2. A new calculation is performed to determine which identities should receive new access rights
3. New access rights are provisioned for the identities in scope

CREATE NEW, MODIFY, AND TERMINATE CONSTRAINT POLICIES

Organizations need to establish safeguards to prevent end users being granted access to multiple systems that could enable them to commit fraudulent activities. If this is not possible due to, for example, not having enough employees in a department to split activities, then a complete audit trail needs to be in place, so risk associated with allowing a potentially toxic combination can be justified.

Process description

The manage constraint policy processes are used to create, modify, and delete constraint policies such as segregation of duty (SoD). These policies are checked each time a user submits a self-service access request, or an automated assignment is made. If there is a policy violation, then the access is not granted, and the issue is escalated to managers, to determine an appropriate resolution.

Best practice IGA system functionality

The process is used to set up access restriction combinations based on business processes or resources. Such constraints prevent access being granted to systems that could be used to carry out fraudulent activities. If a potentially toxic access combination is detected, the new access rights will not be granted, and the issue will be escalated using a predefined workflow, so a resolution can be found. The resolution could involve a manager rejecting or approving access to a system with an appropriate justification as to why the constraint has been manually overridden. The modify constraint policy and terminate constraint policy processes change and delete the constraint policies to reflect business requirements.

Technical process flow

1. The administrator creates a constraint policy and defines either a toxic business process, resource, or attribute combination
2. A new calculation is performed each time there is a potential change to access rights for an identity
3. If no constraint policy violation is calculated, then the access is provisioned
4. If there is a constraint policy violation, the access is not provisioned, and the request is escalated for further action

! BEST PRACTICE...

Define roles and constraints in business terms rather than in technical terms, so the relevant business units, such as finance or legal, can determine if requirements are appropriate.

Process Group
Manage Context

Enables organizations to quickly and easily assign a set of access rights to users who share the same business situation and access needs.

CREATE, MODIFY, TERMINATE, REQUEST AND APPROVE, PROLONG, AND REMOVE CONTEXT ASSIGNMENTS

When users have equal access requirements due to being in the same business situation, contexts allow administrators to manage them as a single entity when assigning access rights rather than inefficiently working on them individually.

Process description

The manage context processes which include create, modify, terminate, request and approve, prolong, and remove context allow administrators to manage the grouping together of users with the same access requirements. These logical groupings can be based on any business situation such as all employees located in a single location or all employees working on a single customer project. Context groups make it easy for organizations to manage user access rights as changes can be made at the context level which is then cascaded to all context members.

Unlike roles which are based on a user's job title, contexts allow greater flexibility as any user can be added if required.

Best practice IGA system functionality

Administrators create a context using the create new context process. Once created, a user can request membership of the context and, if the request is approved by the context owner, be granted all its access rights. These actions are carried out using the request and approve context assignment. Administrators can use existing data fields such as the location of an employee or can create their own and use it as context. Each context can have one or more owners who are responsible for managing those who are assigned to the context.

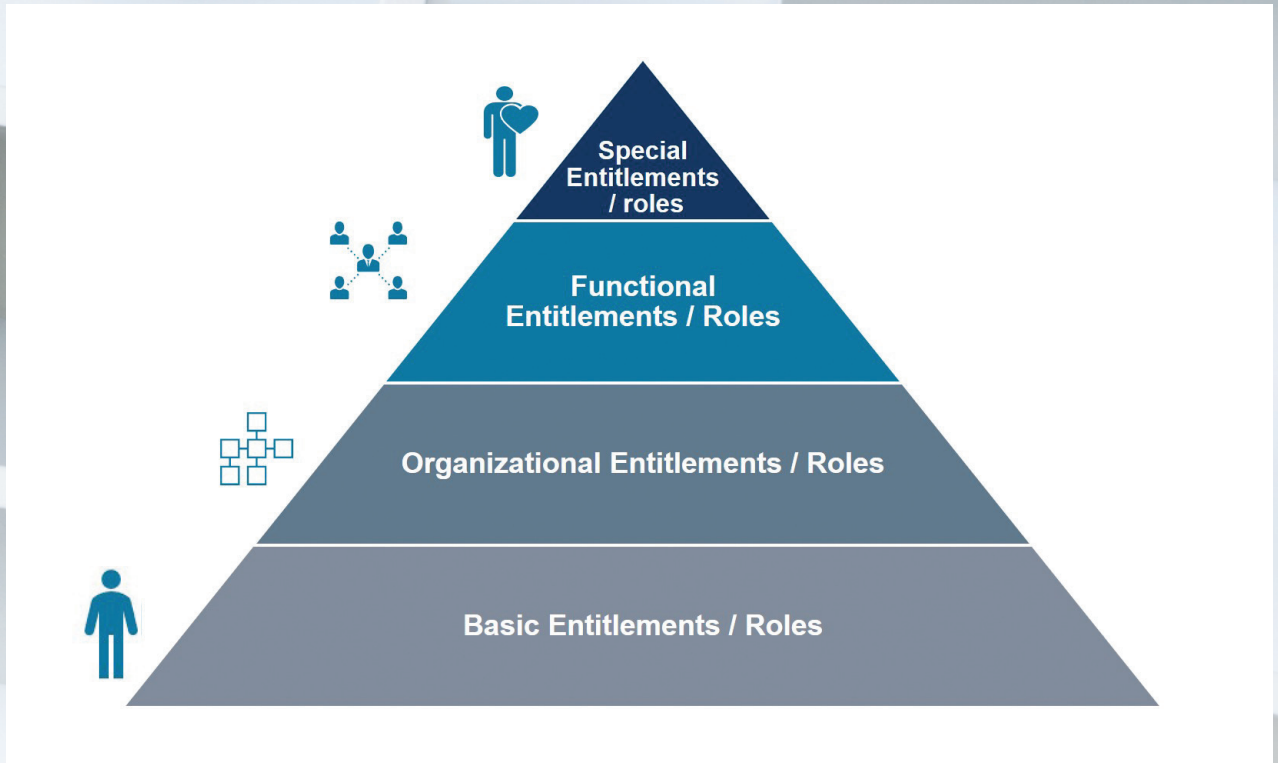
Context owners can also modify the context assignment or delete it as required.

Technical process flow

1. A business context is created by the context owner
2. A user requests access to join a business context
3. The context owner receives a work item to evaluate the membership request
4. The request is either approved resulting in the user joining the context or rejected resulting in the request being discarded

Implementing Best Practice
Business Alignment

To successfully perform business alignment, line managers must work with business system owners to define roles, policies, and contexts which are used to quickly and accurately grant access rights to individuals as they join the company or move into a different role.



PROCESS STAKEHOLDERS

The business alignment processes are administrative processes that make the use of the IGA system easier to use for end users and line managers. The definition of roles, policies, and contexts is carried out by the line managers in conjunction with the business system owners. HR needs to be involved to help ensure that job titles are consistent across the organization so that consistent access can be granted.

Stakeholder	Involvement	Why are they involved?	Pre-implementation tasks	Post-implementation tasks
Human Resources (HR)	HR ensures consistency of job titles in the HR system.	The job titles in the HR system need to be consistent so that the same levels of access rights can be granted to employees with the same jobs.	Ensure consistency of job titles for employees with the same job roles.	Maintaining consistency of job titles as new employees join the company so they can be granted access to the same systems as their peers.
IGA Team	Create the roles, policies, and contexts once they are defined by the line managers	The IGA team are responsible for creating the roles, policies, and contexts in the IGA system once they have been defined by the business.	None	Ongoing creation of roles, policies, and contexts as they are defined and requested by the business.
Line Managers	Help determine the different roles within their teams as well as policies and contexts across the wider organization.	The line managers are responsible for the business and therefore know what information they need to support the granting and revoking of access rights.	Work with HR to ensure that job titles are consistent across job roles. Line managers must work with peers in other departments to ensure consistency across the entire organization.	Ongoing definition of roles, policies, and contexts to match changing business requirements.
End Users	End users do not have any direct involvement in the business alignment processes. However, they are the ultimate beneficiaries as the alignment helps the IGA team and line managers to grant access to them quicker and easier.	None	None	None
Business System Owners	Business system owners work together with their peers and line managers to define toxic access combinations so that constraint policies can be defined.	The business owners and line managers are in the best position to determine which combinations of application access could result in employees being able to carry out fraudulent business activities.	None	1) Determine toxic combinations on an ongoing basis as each target system is added. Work with the IGA team to get policies for toxic combinations created in the IGA system 2) Classify resources 3) Define approval requirements for access requests per resource or system

Key Best Practice Recommendations

Below are a set of key best practice recommendations that should be taken into consideration when implementing the Business Alignment processes in IdentityPROCESS+.

ROLES

Establish role governance process and board or function

To successfully use a role-based model to grant access rights to individuals, it is necessary to have a well-defined set of roles. This is a challenge for many organizations as this task does not always belong to the IGA project. If an organization has decided to use a role-based approach to grant access, but the role model is not sufficiently developed, the IGA project will be delayed until it is in place. In addition, it is important that the role model is not too complex as this makes defining segregation of duty rules difficult.

Ensure that role names are understandable by end users

To speed up the process of granting access rights, roles need to be clearly named so that employees can find the right role to match their requirements without having to call the help desk for support.

Create roles that support compliance requirements

Organizations need to ensure that the roles they have defined can easily fit into a compliance matrix without making it too extensive and complex. Too many diverse roles introduce unnecessary complexity which makes compliance management difficult.

CONSTRAINTS

Define constraints at the role or business process level

Constraints between roles should be defined at a role level or a business process level as this allows organizations to maintain a good oversight and understanding of potential violations. Constraints should be defined in business terms rather than in technical language so that the relevant departments, such as finance or legal, can ensure that the requirements have been defined correctly.

CONTEXTS

Ensure that access rights associated with contexts are removed when a user is no longer associated with it or when it is deleted

Users are granted access rights when they are assigned to a context. It is highly recommended that these access rights are automatically revoked when the user is no longer assigned to the context. For example, if a user is assigned to a short-term project and granted access rights accordingly, their access rights should be revoked automatically when they are no longer working on the project. This ensures compliance and security regarding the access to the project's business systems. In addition, if the context is removed from the IGA system, then all access rights that were granted to users because of being associated with that context should also be removed

Business alignment questions to consider:

- Are roles defined so that they match business needs?
- Are role names understandable to end users?
- Are roles clearly defined to support compliance requirements?
- Which assignment and constraint policies are required by the business?

Summary

Business alignment processes make it easier for organizations to manage users by allowing them to be grouped into groups based on either the jobs they do (roles), the common parts of their jobs such as belonging to the same project group, or based on certain attributes that they share such as belonging to the same department.

Being able to manage users based on certain criteria not only improves the efficiency of the IT department as they no longer need to create access rights for employees individually, but it also increases security and compliance as specific access rights can be defined centrally once and adopted by all users with the same requirements.

Process Area
Identity Security Breach Management

When an organization suspects that a user's identity has been compromised, it is important to act quickly to limit any damage. If the company has not automated their identity security breach process, the IT department may end up spending valuable time creating an overview of which access the identity has and locking these down individually in the relevant business system.

To address this, the following processes are included in the identity security breach management processes:

1. Give administrators the ability to suspend all accounts associated with an identity
2. Allow the administrator to reactivate the access once the situation is under control

The first step quickly stops an attacker from continuing to perform any network reconnaissance, stealing confidential or sensitive data, or causing disruption to operations by corrupting data or making critical business systems unusable. In addition, suspending breached accounts gives the company time to perform a technical investigation and to deal with the non-technical aspects of critical security incidents such as internal and external communications management, protecting the company's reputation and brand, and fielding external calls from customers and the press.

The second step ensures that once investigations have established the causes of the breach and the security administrators have taken the necessary steps to ensure the breach will not reoccur, the locked identities can be quickly reactivated so that business operations can continue.

Why identity security breach management is important:

1. To limit the loss or corruption of sensitive data
2. To limit lateral movement through the network by an attacker
3. To enable automation of an emergency lockout due to information from other security monitoring tools

The IdentityPROCESS+ framework allows the identity security breach processes to be initiated manually. In addition, companies can also implement more advanced solutions by having the emergency lockout triggered by an external security solution such as a security information and event management (SIEM) system, a user and entity behavior analytics (UEBA) system, or a threat analytics solution. As this process is automated, the emergency lockout takes place quicker resulting in greater protection of the organization's infrastructure.

The Identity Security Breach process area includes the following process groups and sub-processes:

Suspend Access

- Emergency lockout
- Revoke emergency lockout

Process Group
Suspend or Reactivate Access

Enables administrators to quickly disable user accounts that they suspect have been breached and to re-enable accounts once investigations are complete and remedial actions have been implemented to prevent a repeat of the incident.

EMERGENCY LOCKOUT

Organizations need to be able to quickly disable user accounts belonging to an individual if they suspect that one or more of them have been compromised to prevent attackers from continuing to perform network reconnaissance, steal confidential or sensitive data, or cause disruption to operations by corrupting data or making critical business systems unusable.

Process description

In the event of a user account being compromised, the emergency lockout process is used to set an identity to “locked” which disables access to all systems for that identity. To reduce the time to implement the lockout, this process shortcuts the need for permission from the employee’s manager which would be the normal procedure. As a result, it should only be used in emergency cases or if requested by authorities and therefore a process should be defined in written company policies.

Best practice IGA system functionality

A manager or operation administrator starts the emergency lockout process in the IGA system and selects the identity they want to lock. For auditing purposes, they must input a reason why the identity is being blocked. The IGA system sets the identity to “locked” and assignment is set to “disabled”. While an identity is set to “locked”, the status cannot be overwritten by any external interface.

Technical process flow

1. A suspected security breach means that immediate action is required.
2. A manager or operation administrator starts the emergency lockout process.
3. Managers can block any of their managed identities and must input a reason for auditing purposes
4. Operation administrators can block any identities and must input a reason for auditing purposes
5. The chosen identity is set to “locked” and assignment is set to “disabled”

REVOKE EMERGENCY LOCKOUT

When an emergency lockout for an identity is no longer needed, managers and operation administrators need to quickly unlock the identities, so users can access their systems to continue working.

Process description

Once the situation causing an organization to lock out an account has been resolved, managers and operation administrators can reactivate the locked identities. This will reenable previous access to all target systems for the identity.

Best practice IGA system functionality

A manager or operation administrator starts the revoke emergency lockout process in the IGA system and selects the identity they want to unlock. For auditing purposes, they must input a reason why the identity is to be unblocked. The IGA system then sets the identity “unlocked” and the assignment parameter is set back to “active”.

Technical process flow

1. The suspected breach is either discounted or the security situation resolved
2. A manager unblocks the identities that he / she manages, or an operation administrator unblocks any locked identity
3. A reason for the unblocking is given for auditing purposes
4. The identity is set to “unlocked” and assignments are set to “active”

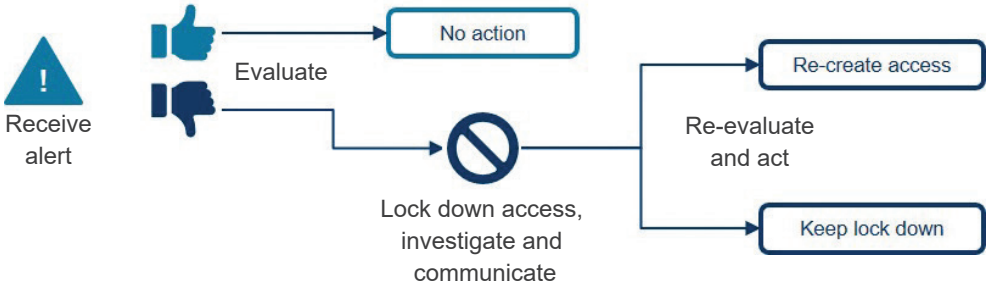


Fig. 6: Simplified identity security breach management

! QUICK WIN...

Good governance:
Be ready to enforce identity security breach policies and start the emergency lockout procedure instantly if an incident is suspected

Implementing Best Practices
Identity Security Breach

PROCESS STAKEHOLDERS

The identity security breach processes are started by the IGA team as they are trained to understand the implications of the emergency lockout procedures. Due to the nature of the potential incidents that could trigger the processes (e.g. employees misusing computer resources), HR needs to ensure that there are policies in place and that they are followed during any suspected incident.

Stakeholder	Involvement	Why are they involved?	Pre-implementation tasks	Post-implementation tasks
Human Resources (HR)	Need to ensure that HR policies are being followed.	As the Identity Security Breach processes may involve locking out users due to misuse of company resources, HR need to ensure that all policies are being followed.	Ensure that written policies are in place to govern the identity security breach Processes	Be ready to enforce the identity security breach policies.
IGA Team	The IGA team will start the emergency lockout process when a security breach or computer misuse internally is suspected.	The IGA administrators are trained to understand the implications of starting the emergency lockout procedure. They also understand what needs to happen to prevent additional breaches or to follow up with employees before access can be restored.	Receive training about the implications of starting the emergency lockout procedure and restoring user access.	Be ready to start the emergency lockout procedure if an incident is suspected.

Key Best Practice Recommendations

Below are a set of key best practice recommendations that should be taken into consideration when implementing the identity security breach processes in IdentityPROCESS+.

Create a written policy for the security breach process

The use of the security breach process must be considered carefully as it involves removing access from individuals. The possible negative implications of using this process includes unnecessarily restricting a user's access to critical business systems or resources due to a suspected external or internal security breach, thus preventing users from carrying out their job.

However, as there are instances when disabling a user's access is legitimate - such as when a security breach is detected or when inappropriate use of the systems is evident - there are times when this process needs to be used. Therefore, it is important for the organization to have a formal policy governing how this process should be used and what should be taken into consideration.

Ensure limited exposure to the emergency lockout

As the reasons for performing an emergency lockout can be sensitive - such as a security breach or a dishonest employee - organizations should put measures in place to limit the number of people who knows about the incident. If the suspicion turns out to be incorrect then this will limit internal speculations as well as any breach of personal confidentiality. If the reasons for the emergency lockout turn out to be correct, then any necessary actions such as internal disciplinary procedures or criminal investigations will not be influenced by speculations.

Identity Security Breach Questions to consider

- Is the security breach policy written down?
- Which stakeholders should be involved?
- Is there a process to limit who knows about the triggering of the security breach process?
- What is the process to roll back the emergency lockout in the event of the initial suspicion being incorrect?

SUMMARY

The Identity Security Breach processes make it easy for administrators to temporarily disable user access when they suspect that the accounts are being used for malicious purposes either by the users themselves or by an external attacker. As this is a powerful process, it needs to be handled carefully and the implications of using it need to be documented and understood by anyone who could use it.

Process Area
Governance

Today it is not enough for organizations to be compliant with external regulations and internal policies. Public cases where companies have had to disclose that an attack may have happened, or data may have been breached, show that proving compliance is a cornerstone in any security operation.

For many companies, it is a very complex task to document who has access to what and why they were granted the access. One possible way to do this is to ask managers to verify their direct reports' access. However, while this is a sensible approach, managers may end up "rubber-stamping" access approvals, simply because the list can be very overwhelming, and they may not be close enough to daily operations to know exactly what access each of their employees need to perform their daily work.

Provide access visibility

The processes in the Governance process area allow organizations to verify who has access to what information, remove access that is no longer required, produce real-time and historical audit reports to provide visibility of access, and ensure that segregation of duty policies are properly enforced.

The process area consists of several process groups targeting different aspects of governance.

Why governance management is important:

1. Ensures that users are not granted more access rights than they need to do their jobs
2. Gives business system owners and line managers the opportunity to ensure the correct level of access
3. Enforces policies involving data protection regulations and access right conflicts

Managing Governance

Ensuring account security and compliance

Access rights that are granted to users, either when they join a company or when they request new access rights, may not be required for the entire employment lifecycle. If the access rights are not evaluated on a regular basis, users typically accumulate access to more systems than they need. The governance processes let administrators verify with the business system owners or employee line managers that the access users have is appropriate for their current jobs.

If an account is found to have no owner assigned to it (a so-called 'orphan account') because an employee has left the company, then governance processes allow for the ownership to be reassigned or for the account to be deleted as appropriate.

In addition to managing access to systems, access to different types of data needs to be controlled. The governance processes allow administrators to ask data owners and managers to assign different risk classifications to data held within their systems. Once these classifications are assigned, data access can be governed in accordance various global data protection regulations and other relevant data protection standards.

Maintaining ongoing compliance

Verifying that the actual state of access granted to users matches the desired state that defines a compliant and secure system is a key process to maintaining good governance. If inconsistencies are found, they are flagged to the administrator, so they can be resolved either by approving or revoking the access.

In addition, the governance processes include workflows to manage segregation of duty (SoD) rules so toxic combinations of access rights are not assigned to an individual, thus preventing the ability to carry out fraudulent activities.

The Governance process area includes the following process groups and sub-processes:

Generate report

- Reporting

Perform attestation

- Design certification campaign
- Administrate certification campaigns
- Respond to campaign questions
- Transfer ownership
- Account ownership
- Access review for managers / resource owners

Perform reconciliation

- Reconcile expected state versus actual state

Apply data classification

- Administer classification tags
- Apply classification tags to data objects

Segregation of duties (SoD)

- Evaluate violation

Process Group
Generate Report

Allows visibility into access rights across all business systems within the organization to ensure ongoing security and compliance.

REPORTING

Having visibility of access rights across all business systems throughout an organization is key to ensuring security and compliance. Real-time dashboards allow organizations to understand their current access compliance situation, so they can act on any compliance violations. Historical reports allow them to prove compliance for auditing purposes.

Process description

The reporting process extracts historical data from the data repository to show information about relevant objects. The reports provide a comprehensive data overview to allow organizations to answer questions such as who has or had access to what, why, when it was granted, who approved it, and when it was revoked. Violations of segregation of duty policies will also be reported. Audit-ready reports enable on-demand access to reports and documentation for auditors which include insights into the logging of processes and approvals.

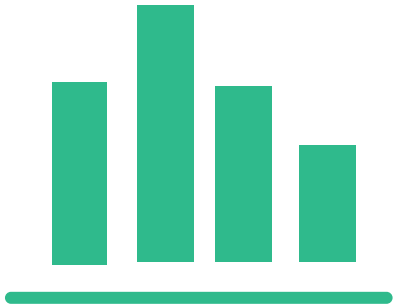
Best practice IGA system functionality

Data is extracted from the IGA system data repository and is used to generate different reports depending on the business requirements. Configurable dashboards are used to display live data showing KPIs (current figures compared to thresholds) and other real-time charts, list views show current lists of data objects, and data warehouse reports are used to generate historical information for auditing purposes to show who had access to what at any point in time.

List views can be downloaded to CSV or PDF for reporting purposes.

Technical process flow

1. A user browses to a relevant report and enters any optional parameters such as time, identity, system, and resource
2. The system verifies that the user has permission to read data from the database and presents the data in the report
3. The user saves the report in Excel, CSV, or PDF to share with others



Process Group
Perform Attestation

Enables companies to ensure ongoing compliance by asking managers and resource owners to verify that the actual access rights that users have for business systems are still valid and by making changes as necessary.

DESIGN CERTIFICATION CAMPAIGN

To ensure ongoing security and compliance, it is necessary to regularly verify that information such as access rights, policies, role definitions, and master data held in an IGA system is still valid.

To succeed, the processes used need to be as simple and efficient as possible to create, so they are not seen as an unnecessary burden by those implementing them.

Process description

Certification campaigns - which are also referred to as reviews, attestations, or re-certifications - are used to periodically validate information held in the IGA system. As well as out-of-the-box certification campaigns, the design certification campaign process allows administrators to define their own.

How it works in the IGA system

The administrator defines the purpose of the campaign including what data is to be certified, who should certify it, and how often the survey should run in the IGA system. The administrator also inputs what should happen when responses are submitted or when answers are not given as well as the notifications and reminders that should be sent, and determines who can monitor and manage the campaign. Once the administrator has set up the campaign, a test can be run in the IGA system and, if necessary, perform any modifications.

Technical process flow

1. The parameters for the certification campaign are determined
2. The certification campaign is created
3. The certification campaign is tested and modified if necessary

ADMINISTER CERTIFICATION CAMPAIGN

Managing certification campaigns involves launching them, performing general administration, and closing them down once they are complete.

Process description

A survey administrator initiates and assigns surveys to relevant managers or system owners. Administration includes determining when the survey should start, monitoring the progress, reassigning questions if requested to do so by the respondent, generating and sending reports to stakeholders, and closing the survey.

Best practice IGA system functionality

The IGA system provides administrators with an interface allowing them to launch the survey created in the design certification campaign process. It also allows them to add information, view the status of survey responses, close the survey early before all questions have been answered if they are no longer relevant, and generate reports.

Technical process flow

1. A survey created in the design certification campaign process is scoped based on factors such as risk classification, systems, and resource types
2. The survey is generated and verified
3. The survey is launched
4. The survey can be optionally closed by the administrator if questions are no longer relevant
5. Once the survey respondent has answered all questions, the survey closes and is set to complete and system actions set up by the administrator are run
6. A PDF report is generated by the administrator

RESPOND TO CAMPAIGN QUESTIONS

Information stored in the IGA system needs to be updated and validated by line managers or system owners to ensure that decisions are made based on the most up-to-date and accurate information.

Process description

After a campaign has been initiated by the survey administrator, all the questions are assigned to individuals, so responses can be given. Questions that cannot be assigned automatically are manually assigned by the survey administrator. A task is sent to the responder, so they can answer the campaign questions.

Best practice IGA system functionality

When the campaign has been launched by the administrator, a task is sent to the manager for review. The system does not require the manager to answer all the questions at the same time and shows a progress bar to indicate how much is left to complete.

Technical process flow

1. The reviewer receives a task to recertify data (e.g. access rights for managed identities)
2. The reviewer reviews the data
3. The reviewer submits answers to the questions and optional comments
4. If the reviewer is unable to answer some of the questions, they can be reassigned to others, if this has been permitted by the administrator. If the survey administrator has not allowed to reassign survey questions, the reviewer can ask the administrator to reassign questions

TRANSFER OWNERSHIP

To ensure ongoing operation and compliance, objects that are left without an assigned owner when an identity is terminated need to be reassigned to another identity.

Process description

When an employee or contractor leaves the company and their identity is deleted, the organization must transfer the ownership of objects to another human identity. This process automatically starts a workflow, which allows resource owners to propose new owners, who can then accept or reject the proposal.

Best practice IGA system functionality

The transfer ownership survey starts as soon as an identity is deleted, and the assignees are calculated based on the type of each of the objects. The survey manages the ownership for technical identities, human identities, organizational units, resources, resource folders, and systems. When the new object owner is proposed, and they accept the proposal, the IGA system makes the change.

Technical flow

1. The identity is terminated
2. A survey is triggered to transfer ownership of objects
3. New owners are proposed
4. The new owner for each object accepts the proposal
5. The ownership of the object is changed

ACCOUNT OWNERSHIP

To ensure compliance, it is important that all accounts have an owner assigned to them. If the rules in the IGA system cannot identify an owner from an orphaned account, then a new owner needs to be assigned manually.

Process description

If the data quality within the IGA system is not sufficient, and defined account ownership rules do not cover all accounts in the target system, it is necessary to manually define an owner for an orphaned account. The account ownership process allows for both the manual proposing of new owners for the orphaned account and for the start of deprovisioning activities in cases where the orphaned account is no longer required, because the owner has left the company. Once the process is complete, the orphaned accounts will either have new owners or will be deleted.

Best practice IGA system functionality

The IGA system displays the orphaned accounts and allows the system owner to start the account ownership process. The system owner proposes new owners for each of the orphaned accounts.

A question is sent to the proposed owner as a work item to give them the opportunity to accept or reject the ownership. The “manual match” is recorded in the master database indicating that the assignment was not determined by rules within the IGA system.

Technical process flow

1. System owner starts the account ownership process and reviews the orphaned assignments
2. System owner initiates an account ownership review
3. System owner proposes a new owner for the orphaned accounts
4. The proposed account owner accepts or rejects the ownership of the previously orphaned account

ACCESS REVIEW FOR MANAGERS / RESOURCE OWNERS

It is good practice to regularly review the access rights assigned to all identities being managed. If a reviewing manager determines that access rights are not appropriate, then they should be removed from the user to maintain high levels of security and governance.

Process description

Access reviews are initiated either on a scheduled basis or manually by system owners, data or system administrators. They can verify accounts by system, organizational unit, specific resources, compliance status, or accounts based on classification tags. When the manager or resource owner receives the recertification survey, they decide whether the user access should be kept or removed from the specified identities.

Best practice IGA system functionality

The IGA system sends the survey request that is either triggered based on a schedule or by a system owner, data or system administrator to the reviewing manager. The reviewing manager can select to keep or remove the access from the identities.

Direct assignments will be expired and deprovisioned immediately. If a kept assignment already has an desired state, then it will remain as-is and those without a previous desired state will get an assignment verdict of the desired state.

Technical process flow

1. A survey is triggered either based on a set schedule or by a system owner or data/system administrator
2. The reviewing manager submits answers to the survey questions
3. Direct assignments or assignments with only an actual reason will be immediately expired
4. If an assignment that did not have a desired state assigned to it is kept by a manager or resource owner, then it will be assigned a desired state
5. Any expired assignments will be deprovisioned

Process Group
Perform Reconciliation

Highlights any discrepancies between the organization's desired security and compliance requirements so that administrators can take necessary action to rectify.

RECONCILE DESIRED STATE VERSUS ACTUAL STATE

To ensure that the desired levels of security and compliance required by the organization are preserved, it is necessary for the IGA system to check that the desired security and compliance state matches the actual access granted to system resources. If there is a mismatch, then the differences need to be rectified to maintain security and compliance.

Process description

The Reconciliation process compares the actual state of the target systems - the current access rights for each business system - with the desired state - the ideal description of security and compliance for the organization. The differences are reported to the administrator, so they can be reviewed, and appropriate steps can be taken.

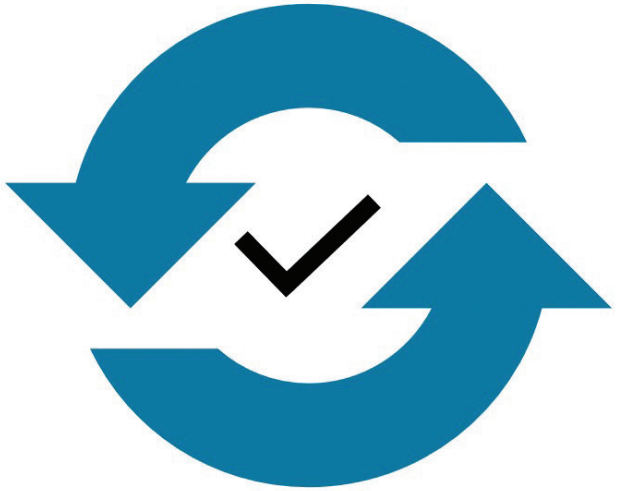
Best practice IGA system functionality

The IGA system compares the defined desired state with the actual state gathered from the target systems and graphically displays the compliance status.

The compliance status indicates whether an assignment is "under control" - i.e. whether it has been explicitly or implicitly approved. Other compliance states could include; not approved, orphan assignment, pending deprovisioning, in violation, or implicitly assigned.

Technical process flow

1. The administrator creates the 'desired state' in the IGA system
2. The IGA system gathers the access rights (the 'actual state') from the target (business) systems
3. The IGA system performs reconciliation by comparing the desired state with the actual state
4. Any discrepancies between the actual state and the desired state are graphically displayed by the IGA system, so the administrator can act to rectify inconsistencies



Process Group
Systems and Data Store Classification

Enables the classification of resources based on the data they store, so that organizations can apply different policies to ensure different levels of compliance based on internal and external regulations.

ADMINISTER CLASSIFICATION TAGS

Resources need to be managed differently depending on factors such as the type of data being stored, the sensitivity of the information, and any regulations governing their use. Applying classification tags to identities, systems, resources, resource folders, contexts, and other objects mean that they can easily be identified when specific company processes need to be applied.

Process description

Classification tags and classification tag categories (groups of classification tags) are added to object types to help organizations comply with company policies and legislative data regulations. The tags allow organizations to establish a risk management strategy and put relevant risk controls in place. In addition to those that are pre-defined, additional classification tags and classification tag categories can and should be defined to match the type of business and national context that the organization operates in.

Best practice IGA system functionality

The data administrators create a classification tag category in the IGA system which consists of a group of classification tags. For example, the classification category ‘GDPR’ could be populated with the tags ‘personal data’, ‘personal sensitive data’, ‘high-risk data’, ‘medium risk data’ and ‘low-risk data’.

These classifications allow the administrator to manage the different types of data according to their security and compliance requirements.

Technical process flow

1. Applicable laws and regulations are reviewed to determine what data must be classified
2. Data mining identifies the classification categories and tags required
3. The classification categories are validated against the classification objectives
4. A risk assessment of the new classification in relation to the law and regulations is performed
5. Classification owners who can approve the classification of objects are selected.
6. The new classifications are described with respect to business objectives and purpose
7. Classification campaigns for objects that need to be classified are initiated

APPLY CLASSIFICATION TAGS TO DATA OBJECTS

Data owners need to identify the data held in different resources, so it can be managed in accordance with the appropriate levels of security and compliance policies defined by the organization. After classification is complete, organizations can identify the data, so it can be managed accordingly.

Process description

When classification tag categories and classification tags have been set up, data objects are tagged using one of the three surveys - classification survey, resources classification survey, or system classification survey – depending on what is to be classified. These classification tag categories and classification tags are used to establish a risk management strategy and put relevant risk controls in place by applying specific policies to them.

Best practice IGA system functionality

The IGA system allows the security officer to create a survey which is then sent to the user. It then presents the user with a task to classify the survey. Once the survey questions have been completed, the IGA system forwards the classifications for approval. Once approved, the classification tags are added to or removed from the object.

Technical process flow

1. A system administrator or a security officer starts a survey
2. The survey questions are created and previewed
3. The survey is started
4. The users receive a task to classify data
5. The user submits answers to the classification survey
6. The user can request to have the question reassigned by the administrator if they do not feel they are the right person to provide an answer
7. The submitted classification will go to the approver who can either approve or reject the classification

! QUICK WIN...

Support the risk management strategy by taking advantage of classification tags and surveys to identify critical and sensitive data

Process Group
Segregation of Duties

Automatically detects the granting of any toxic access combinations to prevent end users from having inappropriate access to business systems that may potentially enable them to carry out fraudulent activities.

EVALUATE VIOLATION

Automatic evaluation of segregation of duties policies needs to be carried out to ensure that individuals are not granted toxic combinations of access rights that could enable them to carry out fraudulent activities when using the systems, they have been allowed to use.

Process description

The evaluate violation process uses the policies defined in the create new constraint policy process to determine whether toxic combinations of access rights have been assigned to the same person, detects any violations, and allows managers to evaluate the situation to determine whether they should be allowed or blocked.

Best practice IGA system functionality

The IGA system evaluates user identities for violations and, if one is found, a workflow sends a task to the manager for approval. If the manager approves the violation by adding comments and selecting a compensating control, then the access is provisioned once it has been approved by the security officers. However, if the violation is not approved, then no access is provisioned.

If the IGA system detects that a violation already exists due to a new SoD constraint policy being added, then it will not revoke any access as this may impede business operations, but will instead send a task to the manager to approve the violation. The offending access will only be removed if the manager rejects the violation.

Technical process flow

1. Identities are evaluated to detect any potential toxic resource combinations based on the SoD constraints
2. If a detected violation occurs, because a resource has been recently assigned to an individual, the access will not be provisioned until the violation has either been approved or resolved
3. If a detected violation is due to an assignment that had already been provisioned before the new constraint was created, then a deprovisioning task will not be created immediately. The IGA system will postpone actions until the violation is approved or resolved
4. The manager will receive a task to approve the violation. To approve the violation, a reason must be given, and a compensating control selected
5. The user group security officers receive a task to approve the violation. They cannot override the manager's decision, but can reject the task and return it to the manager with a comment
6. Approved toxic combinations will be provisioned or kept, and resolved conflict assignments will be disabled or deprovisioned

Implementing Best Practices for Identity and Access Governance

PROCESS STAKEHOLDERS

Ongoing governance is the responsibility of the IGA team and the business system owners. They need to ensure that access to all the business systems is appropriate on an ongoing basis. The line managers within an organization need to validate that end users should have access to various resources when asked to do so via certification campaigns generated by either the IGA team or business system owners.

Stakeholder	Involvement	Why are they involved?	Pre-implementation tasks	Post-implementation tasks
IGA Team	The IGA team may be requested to generate reports for other stakeholders such as compliance and security teams.	The IGA team has extensive knowledge about the data held in the identity and access data system and is therefore in a good position to know what type of reports are possible.	The IGA team should set up attestation surveys across business systems working with the business system owners.	Ad hoc report generation as required by the business.
Line Managers	Line managers will view reports and respond to access review requests.	Managers may want to ensure that accounts associated with their team have appropriate levels of access. As line managers they are able to respond to access review requests as they know what team members are working on.	None	Ongoing response to access review requests as they are generated by the business system owners.
Business System Owners	The business system owners will use reports to determine who has access to their systems. Generate certification campaigns to verify user access and will respond to access reviews for resource owners. Additionally, they will initiate the account ownership process to review orphaned account assignments and transfer them to a new owner.	Business system owners are responsible for ensuring the security and compliance of their systems. Therefore, they need to ensure that only the right people have the right access and that any orphaned accounts are assigned owners or removed.	Business system owners must ensure that there is a business translation of the technical rights so that line managers can respond to access rights on a business level. System owners should also set up ad hoc or scheduled attestation surveys for their system.	Ongoing management of the security and compliance of their systems by analyzing who has access and managing orphaned accounts.

Key Best Practice Recommendations

Below are a set of key best practice recommendations that should be taken into consideration when implementing the governance processes in IdentityPROCESS+.

Define metrics for a key performance indicator (KPI) model
It is important to determine which KPIs need to be measured, monitored and reported on. For administration of the IGA system, this will include system KPIs such as spare database storage capacity, response times, and resource usage. To monitor use of the IGA system from a business perspective, KPIs such as identities being managed, the number of assignments, and unresolved accounts need to be considered. When considering the KPIs required, it is important to involve stakeholders from the business such as line managers, the compliance team, and external auditors as they may have additional requirements.

When considering KPIs and reports, it is highly recommended that organizations start with the out-of-the-box options provided by the IGA solution rather than reinventing the wheel and creating their own. Most organizations find that the standard reports satisfy most of their needs and therefore only need to create a small number of additional customized reports. The process of determining whether the out-of-the-box reports are suitable for the organization could take up to a year to complete if there are many stakeholders with different requirements.

Determine what kind of certification campaigns are needed
To ensure good governance, it is important to establish a rigorous set of certification campaigns. The frequency of certification campaigns should be based on the criticality of the application and any external compliance regulations that need to be taken into consideration. For example, access to a critical banking application may need to be recertified every 6 months whereas a less critical application such as the HR holiday booking system may only need access recertification every 12 months. When determining the frequency of recertification, the audit team should be consulted as they may have specific requirements.

Define how surveys should be run
To effectively perform user access recertification, organizations should determine how surveys should be run. This includes who owns the surveys, who starts them, and who follows up if they are not answered. When deciding who should manage surveys, political considerations need to be taken into account – for example, a senior executive may not appreciate being sent a reminder from a junior employee for not completing answers to a recertification campaign they have received.

Governance
Questions to consider:

- Is there a key performance indicator (KPI) model in place?
- What kind of certification campaigns are needed?
- Who should be responsible for owning and starting surveys?
- Who ensures that surveys are completed by managers?

Summary

The governance processes enable organizations to maintain compliance over user identities for the entire lifecycle of employment. They allow administrators to continuously monitor for orphan accounts and put measures in place to prevent toxic access combinations causing segregation of duty violations.

To monitor compliance, it is important to define and measure against key performance indicators so that senior management can determine how well the IGA solution and associated processes are doing at keeping the company secure and compliant.

By implementing the IdentityPROCESS+ governance processes, organizations will maintain a secure and compliant organization while being able to effectively support the granting of access rights to end users.

Process Area
Administration

As new business applications are introduced into an organization, it is important that they are integrated into the IGA system, so that the identities and user provisioning can be automated and managed centrally. This is important because it not only increases the efficiency of the identity administrator, but also ensures that policies such as segregation of duty are automatically enforced.

Administration processes provide all the workflows to allow an organization to effectively onboard the new business systems and applications while giving them meaningful descriptions so that end users can find the actual resources they need when making self-service requests. In addition, the setting up of password reset management and password policies are handled by the administration policies.

Managing Administration

When a new business application – referred to as the target system - is deployed by an organization, it is integrated into the IGA system using the administration processes.

Before managers and end users can start to request access to resources via self-service processes or approve access requests, the resources are given a meaningful name to make it easier for users to find relevant business systems and for managers to know what they are granting access to. Once the setup is complete, administrators use the password management administration processes to set up password reset enrollment and authentication as well as overall password policies.

Administration processes provide administrators with workflows to modify the target system resource or even terminate a resource no longer used by the organization.

The Administration process area includes the following process groups and sub-processes:

Managing target systems

- Create, modify, or terminate target system resources
- Onboard application

Password management

- Password policy
- Unauthenticated password reset
- Password reset enrollment
- Authenticated password reset

Why identity administration is important:

1. Allows efficient onboarding of new business applications into the IGA system
2. Ensures that new applications are governed by global policies such as segregation of duty
3. Makes the setting up of password reset management and password policies easy

Process Group
Managing Target Systems

Manages the connection of the IGA system to the target business systems so that the IGA system can centrally manage user access provisioning, changes, and deprovisioning.

CREATE, MODIFY, OR TERMINATE TARGET SYSTEM RESOURCES

Information about the business systems, also referred to as ‘target systems’, needs to be imported into and managed in the IGA system so it can manage user access.

Process description

The target system resource processes allow administrators to connect the IGA system to the business systems, so they can read information such as user access rights from them and write new access rights to target systems.

This initial information is enriched so that the IGA system can function more effectively when implementing processes and rules. Once target system resources are retired from operation, they can be removed from the IGA system.

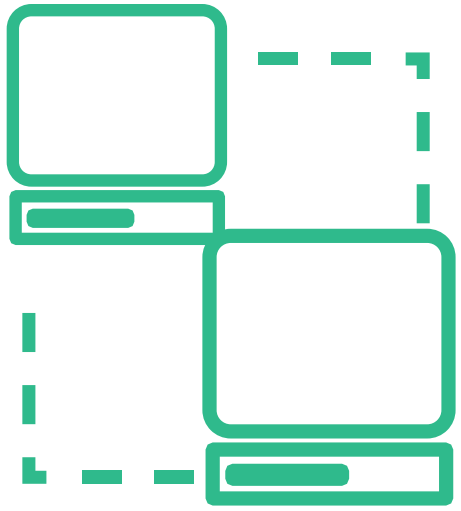
Best practice IGA system functionality

The target system resources are read into the IGA identity and access data systemfrom the connected systems via data collector interfaces. All resources are then created in the IGA server.

Each of the target resources requires enrichment to include data related to ownership, show/hide request access, status and validity, attributes, approval levels, delegation, exclusive management, and post validity. Once this enrichment has been completed, the target system resource can be managed by the IGA system.

Technical process flow

1. Target system resources are read from connected systems into the IGA system
2. Resources are loaded into the data repository
3. Resources are created in the server or the onboard application process is used to create target system resources in the server
4. The administrator or system and resource owners enrich the data in the IGA system



ONBOARD APPLICATION

Enables business applications to be defined in terms of multiple target systems to hide complexity from users requesting access and managers approving or refusing requests.

Business applications often need access to multiple resources which will be unknown to end users. The definition of an end user application needs to be simplified so that all the background complexity is hidden. This allows the user to quickly and simply select a single application they need without any understanding of the technical details which not only reduces the time it takes to request access but reduces the likelihood of errors in approvals by managers.

Process description

Each application may consist of multiple target systems, for example – an application that uses Active Directory for access control would consist of the application itself and Active Directory.

The systems that make up an application are defined, and the application is given a meaningful name and description. These names and descriptions are intended to make it easier for end users to find the applications they want to request access to, and for their managers to understand what they are approving.

Best practice IGA system functionality

The administrator defines the applications in the IGA system based on the multiple target systems it requires.

Once defined, the application roles are enriched with meaningful business descriptions and other attributes that enable end users to find them during self-service access requests.

The application's description and data are verified and approved by an onboarding administrator and are then made available to the access request process by the IGA system.

Technical process flow

1. IT owner of the application starts the process and chooses the system
2. IT owner defines the related physical systems
3. IT owner can define other owners if necessary
4. IT owner selects the business systems from the IGA server or data warehouse to be used in the application
5. The business owner models application roles
6. The business owner can define other business owners if necessary
7. An application onboarding admin approves the modification to the application and related roles

Process Group
Password Management

Enables organizations to manage password policies for each business system as well enabling users to securely reset their own passwords.

PASSWORD POLICY

Password policies for each target business system being managed need to be enforced based on each system's required password strength. Password policies need to be created to ensure that minimum strength policies are enforced to ensure system security across all systems.

Process description

This process ensures that password generation within the IGA system creates passwords that are equal to or stronger than the requirements for the business systems.

Best practice IGA system functionality

The password policy for each business system is described in terms that end users understand so they know, for example, which characters need to be included and how long the password should be. The data administrators create password policies in the IGA system to enforce the minimum strength policies. If necessary, a system owner can make changes to the password policy for the target systems they are responsible for, in order to maintain system security.

Technical process flow

1. Examine the existing password policies for systems where passwords will be generated
2. For each system, define a password policy that matches or exceeds that of the target system
3. Create password policy descriptions to help users when they are creating passwords
4. Data administrators can create and maintain password policies in the IGA system
5. System owners can assign the correct password policy to their target systems

UNAUTHENTICATED PASSWORD RESET

Users need a quick, efficient, and secure way to reset forgotten passwords without having to contact the helpdesk.

Process description

Users that have forgotten their passwords can reset them using a self-service process without having to contact the company helpdesk. This process relies on having the user answer pre-defined questions that they have set up in advance. If they answer the questions correctly then they are allowed to create a new password.

Best practice IGA system functionality

Once the user has entered a username into the self-service password portal, the IGA system checks to ensure that it is an active identity. The user is then presented with several challenge questions, which they must answer correctly. If these steps are completed successfully, the user enters a password.

The IGA system checks that the new password satisfies the password policies of all the systems that are enabled for password reset and then creates sync provisioning requests to perform the resets.

Technical process flow

1. A user that is unable to log in as he/she has forgotten the password, logs in to the self-service password portal and enters a username. This username must be an active identity
2. The user answers a predefined number of challenge questions selected during the enrollment process
3. The user enters a new password, which must match or exceed the strength of the password policy
4. The password is reset in the target systems which have been enabled for reset
5. The owner of the technical identity is informed whether the process was successful or generated an error

PASSWORD RESET ENROLLMENT

Challenge questions are used to ensure that self-service password resets are secure by verifying that the user is who they claim to be.

Process description

The password reset enrollment process allows the administrator to edit the challenge questions available to the user when they are wanting to reset their password. These questions could include questions like “What is your mother’s maiden name?” or “What was the color of your first car?”

The IGA system uses these predefined challenge questions during an unauthenticated password reset to verify that the user is genuine.

Best practice IGA system functionality

The administrator selects the challenge questions within the IGA interface and then can edit those available to end users. The administrator can also set up other parameters, such as the number of questions to be shown, the number of reset failures before the identity is locked, and notification parameters.

If the end user has enrolled for self-service password reset, then he/she will be presented with a set number of challenge questions that can be authenticated during an unauthorized password reset.

Technical process flow

1. The administrator selects which challenge questions they want users to answer
2. The administrator creates new challenge questions if required
3. The administrator defines parameters, such as the number of questions that need to be answered and the number of reset failures that will cause the identity to be locked

AUTHENTICATED PASSWORD RESET

As it is good practice to use different passwords on a regular basis, users need a quick, efficient and secure way to change an existing password without having to contact the helpdesk. Managers or administrators may also determine that users should change their passwords if, for example, they suspect a password has been compromised.

Process description

This process allows users to perform self-service password resets without contacting the helpdesk.

Best practice IGA system functionality

Managers or operation administrators select whose password should be reset in the IGA system and the user is presented with the list of identities grouped by password policy where the underlying system is enabled for password reset.

The IGA system asks the user to enter their current and new password. The IGA system checks that the new password satisfies the password policy and creates a provisioning request to perform a synchronization.

Technical process flow

1. Manager or operation administrators start the password reset process
2. The user selects the accounts that they want to reset
3. The new password, which must match or exceed password policies set for the system, is entered
4. The password is reset for the selected accounts

! BEST PRACTICE...

Enforce recertification of application roles to ensure that underlying target systems are still valid

Implementing Best Practices for Administration

PROCESS STAKEHOLDERS

The administration processes within IdentityPROCESS+ involve the management of target systems, applications, and passwords. The IGA team and the business system owners are responsible for these processes with end users interacting with the IGA system when they need to reset their passwords.

Stakeholder	Involvement	Why are they involved?	Pre-implementation tasks	Post-implementation tasks
IGA Team	The IGA team manages the target system resources in the IGA system.	The IGA team is responsible for managing the target system resources within the IGA system. They ensure that the connections are working properly. The IGA administrators create the challenge questions required for end users to authenticate themselves before they perform a reset if they have forgotten their passwords.	Connecting the target systems to the IGA system.	Ongoing management of the target systems in the IGA system including removing target systems when they are decommissioned from active use.
End Users	End users interact with the IGA system to reset their passwords.	End users may need to reset their password – either because they have forgotten it or because they are requested to on a regular basis by the system owner.	None	None
Business System Owners	Business system owners are responsible for ensuring that enrichment data is added to the target systems and for defining which target system resources define end user applications.	System owners are able to define what levels of approvals are needed, whether access can be delegated, and the password strengths required. Work with the IGA team to ensure changes to the target system, such as upgrades or changes to the APIs, do not affect connectivity to the IGA.	Define which target systems make up the end user applications.	Ongoing recertification of application roles to ensure that the underlying target systems are still valid.

Key Best Practice Recommendations

Below are a set of key best practice recommendations that should be taken into consideration when implementing the administration processes in IdentityPROCESS+.

Enrich target system resources
Although the IGA system pulls in information from the target system, system and resource owners should add additional information, so that processes can run effectively. This information includes ownership of the target system, whether access requests should be shown or hidden, the status and validity of the target system, the approval levels required when granting access to the resource, and whether user access can be delegated to others.

Perform regular recertification of definitions of application roles
Applications and their underlying resource requirements change over time as systems are changed and upgraded. To ensure that the application role definitions are accurate, organizations should regularly recertify them to give resource owners the opportunity to update information about the target systems.

Passwords policies
When creating password policies, complex passwords should be used. As a minimum, the password policy should enforce the use of upper and lowercase letters as well as numbers. If the target systems support special characters, then the password policy should enforce their use as this will increase security by increasing the password strength.

Administration
Questions to consider

- Which approval levels are needed to grant user access to each target system?
- Can access rights to each target system be delegated?
- What are the minimum password strength requirements for each target system?

Summary

The administration processes ensure the smooth onboarding of business systems, so they can be brought under the management of the IGA system. They also allow administrators to simplify the self-service access requests by allowing them to group target systems into a single application that can be understood by end users requesting access rights to them and by managers approving them.

In addition, the managing of password policies and reset procedures mean that organizations can keep control of their security while providing quick and efficient processes for users to reset their passwords.

Process Area
Auditing

Effective audit processes provide reporting capabilities along with operational and management dashboards for identity management and access governance scenarios. This provides IT auditors the ability to understand risks, establish controls, evaluate the existing risks, monitor them, and take corrective action. Examples of such controls are; orphaned accounts, entitlement creep, SoD violations, and visibility into privileged user accounts.

Advanced auditing processes deliver a comprehensive overview of access rights based on identity intelligence from data collected across business-critical systems and applications. Identity and access data is envaulted and compared against policies and any inappropriate access rights or SoD violations will automatically be identified to enable instant remediation actions to be performed.

Reporting, analysis and remediation of actual versus expected state

Analysis and reporting features deliver identity intelligence and answer the basic questions of ”who has access to what”, and “who approved that access”. Auditing evaluates policies for identities, accounts, entitlements, segregation of duties, and privileged accounts against the actual state of identities and access rights, alerting system and control owners of exceptions and supports a timely and orderly remediation.

Validating the expected state of business policies against the actual state of access rights in the applications and systems being managed, warns the administrator, system owners, and security operations of any items or incidents that require attention.

The process groups within the Auditing process area:

- Audit Trail
- Audit History
- Audit Log
- Audit Policies
- Audit Response

Why Auditing is important:

1. To support the creation and evaluation of business policies, rules, and governance controls
2. To monitor the effectiveness of IGA processes
3. To provide assurance to auditors and executive stakeholders that the proper security controls and policies are being enforced
4. To enable the organization to demonstrate that the IT environment is under control and managed properly

Process Group
Audit Trail

Audit trail functionality enables the auditor to gain insight into why access exists and exactly who authorized it and how that access came to be. All customers are subject to one form or another of compliance regulations. This is most apparent for customers within regulated industries or organizations that are ISO certified. They should operate with scheduled and ad hoc security assessments to constantly monitor and alert the responsible teams, if policies are violated or security is potentially compromised.

CIOs and CISO's must ensure that security policies are followed and must be able to provide documentation for the ability to protect sensitive data, and consistently ensure that the organization adheres to compliance requirements across all systems and applications.

Audit trail is a key feature for auditors as it includes processes for documenting:

- Audit trail for all identity decisions
- Audit trail for resource assignments to determine why access has been granted and who authorized it
- Audit trail for resource assignments that have been overridden to determine why access has been given and who authorized it

Process description

The audit trail generates detailed reporting on decisions that have affected resource assignments. The audit trail offers filtering, searching, and sorting capabilities, as well as the ability to drill-down to detailed specific resource assignment reports.

Audit trail reporting and analytics functionality uncovers any improperly assigned access rights or segregation of duty (SoD) violations, and answers – how, why, and when the violation was configured or approved. All decisions for identity entitlement assignments are tracked and available in the audit trail report. Answers given during access approvals, re-certification surveys and SoD reviews are all recorded, and available for reporting functionality.

Best practice IGA system functionality

An IGA solution should provide a consistent level of audit trail data that includes a complete set of information for object changes, changes to permissions, access requests, approvals and custom objects. This level of functionality is essential for auditors and stakeholders who require instant visibility of access rights and need to have the ability to document all aspects of how, when, and why they were granted, including any activity that occurred during access approvals, re-certification surveys, and SoD reviews.

Technical process flow

1. An employee submits an access request stating the reason for the request and the request is recorded
2. The access request is approved both by the manager, and the resource owner of the resource, responses are recorded
3. The access is provisioned, and the audit trail is captured including data on approval, justification, approver, approver role, and time stamp
4. The audit trail is captured and imported into a data warehouse, and exposed in standard reports for further analysis and documentation
5. The audit trail is archived to be available for historical analysis

Process Group
Audit History

History is a key requirement for audit reporting and enables the organization to fulfill the auditor's documentation requirements in a prompt and efficient manner. Auditors should have access to on-demand reports and supporting documentation, including historical data for identity lifecycle processes, access requests, account changes, entitlements, and approvals.

Process description

The History process ensures all historical process data across on-premises and cloud-based systems within the management of an IGA solution. Historical data should be presentable via a dashboard for analytics and exportable in multiple reporting formats for: identities, accounts, resource assignments, policies, and systems.

Historical data should be collected and stored within the IGA solution's data warehouse and archived properly. This will result in the ability to provide a complete overview with compliance relevant statistics. The process should provide a specific date/time-stamp functionality, for documentation of specific actions at any given time. Advanced historical auditing features point in time, changes within period, historical development, and change log reporting.

Best practice IGA system functionality

Any and all objects in the IGA system should enable the auditor to define the search scope and the parameters, which can include: effective times, validity dates, status, categories, and usage patterns based on selected values such as identities, contexts, accounts, resources, resource assignments, orphan objects, account usage, data quality, and systems. The data is extracted from the IGA data warehouse and archive to generate reports. The ability to configure dashboards and custom reporting frameworks can be configured and the data should be exportable in multiple formats for further analytics.

Technical process flow

1. The data object state is stored and available within the data warehouse
2. Each object type, for example account and resource that is imported into the data warehouse, is modelled as a Slowly Changing Dimension (SCD) that tracks the history of the object state
3. Changes to the object state is detected by comparing objects being imported to objects that are already stored in the data warehouse database. Objects comparison is performed at the attribute level
4. If the status attribute on an object is changed, the data warehouse creates a new version of the object with the new version value
5. The history of an object consists of all the tracked versions. Each version represents the object state for a specific point in time, indicated by an effective and expiration time
6. Historic data is displayed from the data warehouse to the dashboard for auditing reporting

Process Group
Audit Log

To demonstrate that an organization is taking the appropriate actions to monitor access and ensure regulatory compliance measures are being adhered to all survey audits must be logged as an assurance mechanism for the auditor to validate that appropriate controls are in place.

Process description

The auditor, system administrator, and relevant system owners have the ability to view assigned survey audits and update them in real time as well as review the reports for continuous evaluation of key controls, business rules, data integrity, and performance.

The auditor should have the ability to verify and prove that a survey audit has taken place in accordance with security requirements, regulatory controls, and business policies, with a date and time log of any remediation actions.

Best practice IGA system functionality

Auditors, data protection officers (DPOs), or system administrators are provided with a dashboard view through the IGA portal. Based on the system administration view the dashboard will allow the auditor or administrator to leverage the various widgets to display information from sources such as the event viewer, application logs, IGA processes, SQL processes, etc.

Technical process flow

1. The auditor or IGA system owner can review all compliance surveys that have been performed by the IGA system
2. Locate the survey additional information is required for
3. Review the details of the desired survey in real time
4. The ability to review responses and export to a PDF for printing is available
5. Repeat this process for all surveys that this level of information is required for

Process Group
Audit Policies

Typically audit policies are aligned with an organization's business rules and then incorporated into the relevant IGA processes. Audit policies should be reviewed on a routine basis to ensure they are effective in providing enforcement and the desired business results. To ensure continuous policy compliance and data integrity the organization should leverage supplementary audit policies in addition to the key controls that are built into the IGA processes.

Process description

Audit policies evaluate business rules and controls against the actual state of identities and associated access rights. In the event inconsistencies or violations are discovered, the process should include a method to alert control owners and include the option to perform remediation actions.

The process includes the ability to perform policy management through an auditing dashboard that displays all audit policies that a user is authorized to view and manage.

Best practice IGA system functionality

Audit policies should be configured to constantly review all active identities and compare the actual versus desired states. This comparison will reveal any inconsistencies to the proper support teams, such as technical accounts without owners, contractor access with missing or invalid expiration dates, roles with conflicting entitlements or violations within segregation of duty combinations, or privileged accounts / entitlements not included in recertification surveys.

CONTROL POLICIES

Used on an ongoing basis to detect and react to inconsistency within the policies. Potential issues include objects that do not have an owner, circularities in the role hierarchy, and roles without proper descriptions and mandatory fields defined. In case of an issue within a policy an audit case workflow is launched and assigned to the policy owner to remediate.

CONSTRAINT POLICIES

Are typically used to detect conflicts or problems within segregation of duty policies. The policy owner should have the ability to override and accept violations after providing a justified reason for the need to implement compensating controls. SoD constraint policies are evaluated every time the access rights for an identity are re-evaluated within the IGA solution.

RISK SCORING

A focused policy used to define the risk to the enterprise for improperly configured control policies and constraint policies. Every improperly applied policy and override of a constraint policy contribute to the risk score.

Process Group
Audit Response

Audit response processes enable the organization to ensure that exceptions are detected and handled by the responsible policy owner who can take corrective action.

Process description

The IGA solution should be configured to continuously evaluate policies on defined schedules or triggered ad hoc by an audit policy owner. Audit response processes are designed to address any policy violations or exceptions that are revealed as a result of the policy evaluation.

Policy violations should be treated as cases or incidents and tracked via an escalation workflow for actionable follow-up and remediation.

Best practice IGA system functionality

When a policy exception is detected or observed, control policies trigger a workflow that alerts the policy owner. Part of the workflow process is to determine if an incident/case already exists for that specific violation/exception and determine whether a new case/incident should be created.

The workflow alerts the policy owner, a user's manager, or information security teams who could have a specific role to determine the correct remediation approach for the incident. Depending on the type of policy violation and exception required, the policy owner may be able to allow, correct, or mitigate the incident or close the case.

Technical process flow

1. Data from target systems are loaded into the data warehouse. History and KPI improvements are monitored
2. Accounts are matched to identity master data and consolidated for a cross-platform view of identities to access risks
3. Changes to the state are detected by comparing imported identity data to the stored data. Relevant exceptions are revealed immediately in the audit report dashboards
4. If the status is changed an exception alert is created
5. The policy owner receives alerts with a list of exceptions
6. The policy owner determines whether the exception is a new or existing, and either opens a new case or overrides the exception
7. The policy owner performs an analysis of the exception and decides whether to remediate, mitigate, or update data depending on the associated audit control policies. Automated exception mitigation processes can be applied
8. Exceptions and actions are logged in the data warehouse to provide a historical perspective

Implementing Best Practices for Auditing

PROCESS STAKEHOLDERS

The auditing processes within IdentityPROCESS+ includes robust auditing capabilities for management of policies, handling of exceptions, and for ensuring a comprehensive audit trail and history for advanced reporting and analysis. The handling, maintenance, reporting and analysis in relation to the processes involve several stakeholders across the organization:

Stakeholder	Involvement	Why are they involved?	Pre-implementation tasks	Post-implementation tasks
Executive Team (CIO, CISO, CPO)	Communicating IGA relevant IT security requirements and objectives	Establishes the vision for effort	None	Reviewe results to ensure audit requirements are addressed properly
Policy Owner	Ensures the policy is aligned with the business to deliver the desired results	Owns policies for their focus area	Communicates business requirements to project team	Participates in reporting and re-certification campaign scoping and follow-up. Determines who will remediate exceptions.
Auditor	Conducts audits	Defines audit parameters	Participates in testing audit functions	Analyzes and remediates exception cases
IGA Team	Configures and monitord the IGA platform	Installs and configures IGA platform	Ensures all IGA prerequisites are addressed	Monitors and makes platform modifications

Key Best Practice Recommendations

Define effective audit processes

It is essential that audit policies are aligned with the business and deliver the expected results. The audit processes should always provide answers to the questions of "who has access to what, who approved that access or policy exception?" Use control policies to detect and react to inconsistency within the policies. Provide a remediation workflow to address any issues discovered within the policies. Leverage constraint policies to detect conflicts or problems within segregation of duty policies and provide a way to document policy exceptions and overrides (compensating controls). Assign each policy object a weight/score and include a risk scoring control to understand the exposure of policies not being implemented or enforced properly. Provide auditors governance dashboards and the ability to report the status of the various policies, and for continuous evaluation of key controls, business rules, data integrity, and performance to ensure each policy object is being historically documented and stored properly.

Establish effective SoD audits

The lifecycle of permissions and roles can be very dynamic. As a result, segregation of duty policies (SoD) can over time become highly complex and difficult to manage. This also can lead to the policies becoming stale or dated, resulting in the generation of false policy application results. Without a business-oriented approach the organization will struggle to deliver effective SoD audits. Therefore, it is recommended to define segregation of duties (SoD) policies based on business processes, supporting the standard approach of roles and permissions.

The list of business processes can be hierarchical, allowing the organization to define both fine-grained SoD but also broader operational constraints. The organization can rapidly introduce new SoD constraints without needing to re-build their role catalogue, since the SoD policy is based on business process that changes much less frequently.

Ensure ongoing compliance

Some organizations implement scheduled security assessments once or twice a year or quarterly, an approach that has the potential to create gaps in security that can go undiscovered for months at a time. In regulated industries and for mission-critical systems, it is highly recommended to conduct audits more frequently. To constantly monitor and alert if policies are violated or security is compromised, policy auditing processes can be set to run as a continuous activity to achieve the following:

- Establish constant controls of access to business-critical data and IP
- Identify and resolve SoD issues
- Ensure that all relevant access rights are identifiable
- Review policies quarterly for effectiveness
- Refine and apply granular reporting and analysis

Auditing
Questions to consider

- Do we have business alignment?
- Who are the designated policy owners?
- How often should the auditing processes be scheduled to run?
- What is the frequency for policy review?

Summary

Advanced auditing capabilities support the business policies and should be included in the organizations' IGA processes. Extending the IGA framework with automated processes for auditing ensures data integrity by detecting and remediating exceptions, so the desired policy results are accomplished. Leveraging in depth reporting, analysis and evaluation of policies for identities, accounts, entitlements, segregation of duties, and privileged accounts provides effective auditing. Automated audit processes provide the ability to compare the actual state of identities and access rights in comparison with the expected or desired state, the capability to alert policy owners of violations and exceptions, and deliver a workflow that facilitates a timely and orderly remediation.

IGA Best Practice Processes
Next Step

AN ONGOING JOURNEY

The diverse areas covered by the processes in the IdentityPROCESS+ framework make it possible for organizations to implement many different functions during an IGA project. However, the large number and variety of processes can initially make it difficult for organizations to know where to start - even if they have an earlier generation of an identity and access management (IAM) solution already installed. In this section, a recommended approach is described to give organizations a starting point from which they quickly can get up and running to demonstrate value to the business.

It should be remembered that an IGA implementation does not have a single destination - there are many different paths that organizations can take depending on whether their key goals are security, compliance, or efficiency driven. Regardless of which path is taken, organizations find that IGA implementations are an ongoing journey as the business they are supporting is constantly changing due to new users being employed, new applications being introduced, mergers and acquisitions, and many other business changes requiring continuous support.

HOW TO GET STARTED?

Determine the goals

When starting an IGA project, it is important to determine the key business goals and not just focus on technical objectives.

Typically, most organizations define goals in the following areas:

- Increasing the levels of security for on-premises and cloud-based applications
- Improving compliance associated with internal procedures and external regulations
- Improving efficiency by making it easier to manage more identities without adding additional employees to the IT organization

Once the overall goals have been determined, organizations need to establish sub-goals to be able to document the success of the project.

Examples of sub-goals are:

- Eliminating all orphan accounts within the organization
- Automating processes around onboarding of new employees and ensure they have the access they need from their first day at work
- Regularly producing a set of audit reports to meet compliance
- Being able to provision all user access requests within a given timeframe
- Being able to report on the reasons for all access policy violations such as SoD violations

Assemble the stakeholders

Once the goals and sub goals have been defined, the IGA team can then bring in the relevant stakeholders to discuss whether the goals are realistic and whether there are other factors that need to be included. As IGA projects typically touch most if not the entire organization, it is important to ensure that a wide representation of stakeholders is included. There should certainly be representatives from corporate security, compliance, auditing, IT, and business managers who understand how applications are used within the organization. To ensure the success of the IGA project, it is critical that these stakeholders are kept up-to-date on the progress of the project so that their ongoing buy-in is assured.

Initial implementation and quick wins

Once the project goals have been established and a group of stakeholders has been brought together, work can begin on the actual implementation of the IGA system. It is important to show some quick wins to the business so that they continue to allow valuable resources to be allocated for the rest of the project.

DEMONSTRATE EARLY VALUE IN THE IGA PROJECT

Importing HR and Active Directory data

As described in the IdentityPROCESS+ processes, an IGA solution needs information from personnel records, so it can perform tasks such as assigning access rights based on roles and route approval requests to appropriate line managers. As a result, the first task that needs to be carried out is to import personnel information from authoritative sources – typically the HR system and any contractor databases – into the IGA system. For this task to be effective, it is important that only high-quality data is imported, which means that organizations should ensure that the data held in the HR system is cleaned before it is imported.

Once personnel data has been loaded into the IGA system, the next logical step is to onboard and import data from Active Directory (AD). This provides the IGA system with additional information about users and will form the first step in getting in control of data.

Get in control of AD accounts

The first quick win that can be achieved during the early stages of an IGA deployment is to enable the organization to get in control of AD accounts. By comparing the current employees and contractors imported from the authoritative sources with the actual accounts in AD, the administrator can quickly establish which AD accounts do not have an owner within the organization. The comparison can be done using automatic built-in rules matching which will show the discrepancies between the data-bases. Using this information, the administrator can determine if the accounts should be assigned a new owner or terminated. This procedure applies to both end user accounts and technical accounts.

Once the organization has gone through this process, administrators can be confident that they no longer have any orphan accounts (accounts in their AD without an owner). This means that they can guarantee that all accounts in their AD are compliant as they are validated and have an owner.

Stay in control by adding more processes

Once an organization has achieved initial control, certain processes need to be put in place, so that they stay in control. These processes are mentioned below and are all included in the IdentityProcess+ framework.

The three governance processes (design, administer and respond to certification campaigns) enables companies to ensure ongoing compliance by asking managers and resource owners to verify that the actual access rights that users have for business systems are still valid and by making changes as necessary.

The onboard identity process ensures that all initial access is created when a new employee is added to the HR system, the onboard contractor process when a new contractor is added, and by the request technical identity when created by a system owner.

The request access and approval of access requests processes ensure that users are only granted access to the systems that they require to do their jobs. This means that the organization can remain in control of who has access to what and why.

Another key part of staying in control involves managing employees as they move departments or get promoted. Implementing the intra-organizational transfer process ensures that employees are granted any additional access rights they need, but at the same time have removed all the access rights they do not need so they do not accumulate unnecessary access rights over time.

When employees or contractors leave the company, the termination process will automate the removal of access rights from all systems they have access to so ex-employees are unable to access business systems.

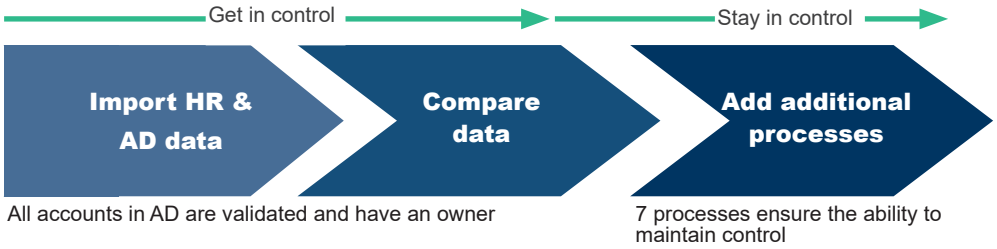


Fig. 7: The steps outlined ensure quick value to the business in the IGA project.

Add applications and business critical systems

In the same way as you want to get in control of your AD, you want to get in control of all business-critical applications. To do this, the application is first onboarded using the create target system resource process and then the access review for managers and access review for resource owners' processes are used to verify whether the user access rights for the applications are appropriate. If a manager or resource owner determines that a user should no longer have access, the access can be revoked. Once in control, the same processes that are used to stay in control of the AD environment are used to manage user access rights as they join, move, and leave.

WHAT'S NEXT?

Once an organization has implemented these core processes to get in control and stay in control, there are many possible paths that their IGA project can take to build on the foundation created and thereby add more value to the organization.

Examples include:

- Expand the use of assignment policies to further reduce manual work
- Build out the role model and use of contexts to reduce administration and create a better experience for the organization
- Introduce B2B identity and access governance enabling B2B partners to get access to the resources they need while you stay in control
- Build out constraint policies such as SoD policies to improve compliance and security
- Automate the emergency lockout process
- Expand the use of certification campaigns to get in control of other data than access data
- Introduce data classification to improve the governance of sensitive data

Implementing any of these additional processes will increase the return on investment of the IGA project. It is recommended that organizations work with their IGA vendor to create and implement a roadmap which will help them match their business requirements and provide the most value to the organization.

IGA
Glossary

Access management
The IdentityPROCESS+ process area that manages access rights for new employees or employees moving around the organization.

Access request
A process for end users to ask their line manager or a resource owner to grant them access to a business system.

Account
A user or technical account in a system – for example, an Active Directory account – that is assigned to or given access to resources (access rights) in a system.

Actual state
Current access rights that users have to business systems. This information is read from the business systems and is used to determine compliance by comparing them to the desired state.

Administration
The IdentityPROCESS+ process area that manages the integration of target systems into the IGA system to allow central administration of user access and governance as well as password management.

Attestation
The process of periodically or on an ad hoc basis reviewing and validating that access rights, policies, role definitions, and master data in the system is correct and valid. The most common certification campaigns survey identity access to resources in target systems.

Authoritative source
The main source of personnel record information that is used by the IGA system to implement rules and processes. In most organizations, the authoritative source will be the HR system as this database holds the most up-to-date information about employees joining and leaving the company as well as their job title and current line manager.

Business alignment
The IdentityPROCESS+ process area that simplifies IGA processes for non-technical users and simplifies the maintaining of access rights for employees with the same job role or those who work in the same business area or participate in the same project.

Business system
An application within an organization that users request access to, so they can do their jobs. Examples could include a CRM system, email, or production database.

Certification campaign
A survey that is sent out to line managers and resource owners to verify information such as access rights, policies, role definitions and master data held in the IGA system.

Classification tags
A method for system owners to identify the types of data held in their applications so that appropriate policies can be applied to them to ensure compliance with internal regulations and external legislation such as GDPR.

Constraint policy
A policy that safeguards against end users being granted access to multiple systems that could result in them being able to commit fraudulent activities due to the levels of access they have been granted. If a constraint policy is violated, then the business should split the access between different employees to reduce the risk of malicious activity. See segregation of duty.

Context
A way of grouping users into organizational units so they can be managed in the same way. A context could, for example, be a group of people who work on the same project, have the same costs center or work in the same factory.

Data administrator
A member of IT who is responsible for planning, organizing, and controlling data resources within the organization.

Data classification
The process where data administrators and resource owners tag the types of data held within the systems they are responsible for. These tags are then used to apply policies to ensure that the data handling conforms to regulations.

Desired state
The ideal access rights that users should have to ensure compliance and security standards are met. This information is compared with the actual state to determine non-compliant user access that requires action by the administrator.

Direct assignments
When an identity uses the standard request access process and has received approval for resource assignments, a resource assignment that is associated with identities is created.

Emergency lockout
The process of quickly disabling all accounts associated with an identity when a security breach is suspected to prevent an attacker from continuing to access an organization's data or preventing business systems from operating.

HR system
A database system used by organizations to manage the day-to-day human resources operations. The HR system is usually the most up-to-date and accurate record of the employment status of the workforce and is therefore used in IGA implementations as the authoritative source.

Identity
The representation, by a uniquely identified object with a defined set of information associated, of a physical person or technical entity whose access to systems must be documented and managed.

Identity lifecycle management
The IdentityPROCESS+ process area that manages the entire employment of an individual from onboarding through their career and finally offboarding when they leave the company.

Identity security breach
The IdentityPROCESS+ process area that manages the emergency lockout and restoration of access to a user account when an organization suspects a security breach.

Master data
Personal information for an employee or contractor such as name, job title, and line manager that is gathered from one or more systems (typically the authoritative source), stored in a central repository, and used by the IGA system for tasks such as enforcing policies and routing access requests.

Offboarding
The process of ensuring that employees, contractors, and other users are no longer able to access an organization's business systems once they leave the company.

Onboarding
The process of ensuring that employees, contractors, and other users are granted appropriate access to business systems when they join the company, so they can do their jobs.

Orphan account
An account that does not have a person assigned to it. This could be because an employee has left the company, but their account has not been deleted, or a technical identity has not been assigned an owner. Orphan accounts should either be assigned an owner or deleted as otherwise they cannot be properly governed.

Policy
A policy defines that a set of identities should have access to a set of role and/or resources (assignment policy) or be restricted from being assigned to certain combinations of role and/or resources (constraint policy). Policies are definitions of allowed or prohibited combinations of identities, roles, and contexts.

Process
A description of a set of actions that describe a discrete task that can be carried out in an IGA system.

Process area
A broad collection of process groups that define the processes to manage certain business requirements using an IGA system. IdentityPROCESS+ defines seven process areas: Identity Lifecycle Management, Access Management, Business Alignment, Identity Security Breach, Governance, Administration, and Auditing.

Process group
A collection of IGA processes whose tasks are related and therefore are logically grouped and implemented together.

Provisioning
The processes that create, modify, and deactivate accounts and privileges across systems. Provisioning can be done manually or automatically through technical integration.

Reconciliation
The process of confirming that all managed target systems accounts and access rights comply with defined policies. For example, the desired state of all accounts in all managed systems and their access rights must be the same as the actual state – i.e. the access rights for the managed systems. Reconciliation should be performed regularly to rectify any discrepancies between the actual and desired states.

Resource
A permission or set of permissions defined in a physical system by that system's access control model. Groups in a directory service, such as Active Directory, are considered as resources.

Resource owner
The administrator that is responsible for the management of a resource.

Role
A collection of resources from one or more systems, or other roles. Roles can be assigned to identities (i.e. this person has this role).

Segregation of duty (SoD)
A principle that ensures that key processes are shared between multiple people or departments to minimize the risk of fraud and errors due to one individual being responsible for a task's execution. IdentityPROCESS+ defines a process to detect the granting of any toxic access combinations and prevents them from being provisioned without specific reasons being given and approval from security officers.

Survey
A survey is a series of questions sent to line managers and resource owners asking them to perform attestation or recertification of user access rights.

System
A technical system such as Active Directory, a finance application, or HR system. One system can represent other systems across access control models.

System owner
The administrator that is responsible for the management of a system.

Target system
A business system that is integrated with the IGA system so that the user access rights can be managed centrally.

Technical Identity
An identity that is used to provide multiple members of the IT team with administrator access to systems without the need to use their personal identities. As these identities have privileged access rights and are used by several employees, they need to be governed carefully to guard against misuse.


SUCCESS
VISION
GOAL
TEAM
ANALYZE
BRAINSTORMING
PLANNING
STRATEGY
IMPLEMENTATION

Since 2000, Omada has focused on using identity to create business value - measurable value, from IT and HR to marketing and sales. Identity, managed the Omada way, simultaneouslyimproves security, efficiency, cost control and regulatory compliance throughout any organization. And, it can do even more. Identity can accelerate digital transformations, smooth M&A integration, and enable deeper relationships with suppliers and customers. Few technologies have the potential to impact so much. Belief in this essential role of identity unites our organization, fuels our innovation, and strengthens our collaboration with partners. We have pioneered many of the best practices in use today and are passionate about taking identity management even further. We are committed to using identity to create business value.

Omada

omadaidentity.com