International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Identity Governance Access (IGA) challenges and Omada IdentityPROCESS+ approach for IGA

Seema Kalwani

seemakalwani@gmail.com, Security Engineer, IL, USA

Abstract
The article provides Omada overview covering different challenges in an organization - lack of security, Non-compliance, maintaining efficiency. How Omada (IGA) solution and its IdentityPROCESS+ approach addresses the challenges through Identity Management life cycle, Access Management, Business alignment, Governance, audit and Administration. Use of IGA with PAM solutions is a common.

Keywords: IGA, Governance, IdentityPROCESS+, Identity Management, Access Management, Audit, Compliance, Regulation, Security breach, identity, Business Alignment, Administration

1. Challenges without IGA

Privileged Access Management (PAM) vaults such as Symantec PAM, CyberArk etc., are used to secure passwords of service accounts in the vault. Identity (Users) to perform their day-to-day operations need the credentials of the service accounts in the vault. The access provided to users (identity) needs to be requested, approved, provisioned. The access management and identity management is provided by Identity Governance Access (IGA). We will look at challenges that IGA resolves and then look at the IdentityPROCESS+ approach to deployment of the same in organizations.

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:

(1) LACK OF ADEQUATE SECURITY
(2) NON-COMPLIANCE
(3) MAINTAINING EFFICIENCY

LACK OF ADEQUATE SECURITY - Organizations struggle to secure that all IT systems – on-premises and in the cloud meet strict identity and access security requirements to avoid security breaches.

A. 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.

B. *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.

C. *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.

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

Fig. 1. Compliance picture from IGA Admin Guide

A. *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.

B. *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.

C. 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.

D. 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 - 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

A. 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.

B. 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, offboarding, 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.

C. 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.

2. 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'.

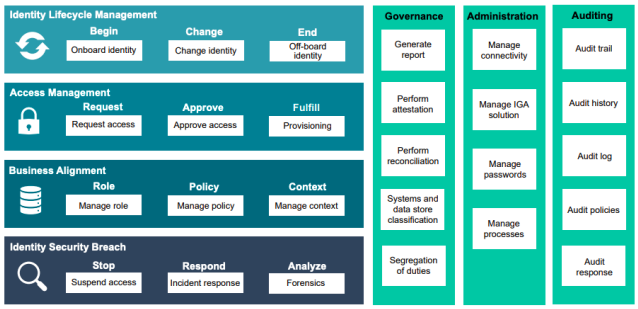

Fig. 2. Identity PROCESS+ picture from IGA Admin Guide

D. 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.

1) 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.

2) 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.

3) Offboard 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.

E. 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.

1) *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).

2) *Approve avvess*

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.

3) *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.

F. 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.

1) *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.

2) *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.

3) 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.

G. 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.

1) 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.

H. 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 employees, 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.

I. 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.

J. 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

1) 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.

3. Conclusion:

IdentityPROCESS+ framework 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

Omada, a global market leader in Identity Governance and Administration (IGA), offers a full-featured, enterprise-grade, cloud-native IGA solution that enables organizations to achieve compliance, reduce risk, and maximize efficiency. Founded in 2000, Omada delivers innovative identity management to complex hybrid environments based on our proven best practice process framework and deployment approach.

References

1. OmadaIdentity, "Omada-Guide_IdentityPROCESS-3.0.pdf", https://omadaidentity.com/wp-content/uploads/2025/01/Omada-Guide_IdentityPROCESS-3.0.pdf (accessed Feb 2025)
2. OmadaIdentity, "gartner-market-guide-iga", https://omadaidentity.com/press/2024-gartner-market-guide-iga/ (August 2024)
3. OmadaIdentity, "Omada-report The state of identity governance", https://omadaidentity.com/wp-content/uploads/2023/11/Omada-Report_The-State-of-Identity-Governance-2024.pdf, July 2024
4. Prnewswire, "Omada introduces role insights to strengthen and simplify identity governance", https://www.prnewswire.com/news-releases/omada-introduces-role-insights-and-analytics-to-strengthen-and-simplify-identity-governance-302303527.html, Nov 2024

5. Seema Kalwani, “Symantech PAM (Privileged Access Management) features enablement security audit compliance regulations”, IJIRMPS Volume 13, Issue 1, January-February 2025, doi: 10.37082/IJIRMPS
6. Stephen Lowing, “Identity-governance-drivers”, https://www.idsalliance.org/blog/identity-governance-drivers-in-the-2nd-half-of-2024/, July 2024