eBook

5 IGA Essentials to Support Your Cybersecurity Strategy

Omada

Content

The Complexity of
IT Security Infrastructure

The COVID-19 pandemic has created an entirely new range of cybersecurity risks for organizations and driven digital transformation in a pace unprecedented. Because of the sudden shift to working remotely, organizations saw new threats to home networks and devices, remote access systems, virtual private networks, video-conferencing, and other collaboration tools. What many considered optional became imperative overnight.
New dangers suddenly appeared both internally and externally.

And as a result of this transformation, Identity has now become the best perimeter of defense.

Protecting access to sensitive data, especially for your remote workers is not just about security devices and VPN solutions. It is also about managing who has access to specific data and ensuring that they can only access data that they are entitled to access. While it might not be possible to control the type of device or connection that remote workers use to access data, it is still possible to enforce rules as to the type of data that a specific identity or role can access in a specific situation. In the hyper-connected IT environment identity governance and administration (IGA) has become critical to maintain a high level of security and compliance while ensuring users have the access they need to do their job.

YOUR DATA IS YOUR BUSINESS

Operating an efficient business today requires users to have easy access to a multitude of IT systems, applications, and data located in the cloud, the datacenter, or some combination of the two. Sensitive data and information getting into the wrong hands, can result in severe damage and huge risks to a company. And this risk has expanded as sensitive data is shared more and more with contractors, suppliers, outsourcing providers, and other users. Breaches within this complex web of access can mean disclosure of sensitive information such as patents, business forecasts, personnel data, privacy data, innovations, and other important assets. Your data is your business.
This is where Modern IGA can secure access to your data across all your platforms.

KEEP UP WITH CHANGE

Every day, technological development changes business. New personnel and capabilities come online. New opportunities appear and with them, new threats. Each of these changes brings new requirements for IGA, whether it's the simple addition of a new employee or launching an entire line of business. Governance processes and access management must have a response ready to deploy simultaneously. If not, every change is another chance for breach or error. With the journey to the cloud, the need for both agility and security is even greater.

AVOID THE NEXT BREACH

Security is not just a question of controlling the access rights of individuals. You also need to consider the mix of on-premises and cloud-based applications we now use every day as well as all the different user identities individuals have on a variety of platforms. With all these variables, you can start to see how complicated the challenge can get. To avoid these security risks, organizations need to control the management of user identities and their access to resources and cloud services.

GET MORE DONE

Business velocity, delivery cycles, agility—call it what you will, success in digital business (which now means all business) relies on constantly increasing efficiency - and security. With Modern IGA that provides both powerful governance of access and a flexible environment, IT organizations can increase employee productivity. How? Through the automation of life-cycle processes such as on-boarding, off-boarding, and departmental change processes for employees, business partners, and customers across hybrid infrastructures. It also ensures employees, partners, customers, and contractors have the access they need, exactly when they need it - without costly delays.

"The negligent insider is the root cause of most incidents. Specifically, of the 4716 incidents reported:

2962 were due to negligent or inadvertent employees or contractors

1105 were caused by criminal and malicious insiders

649 involved stolen credentials

191 involved the theft of privileged users' credentials"

From IBM Security Cost of Insider Threats Global Report 2020

Cybersecurity
Identity has become the Perimeter

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 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 security breaches include 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 and industry-specific regulations.

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

Cybersecurity threats include:

- Theft of intellectual property through compromised accounts from social engineering or online attacks
- Fines for noncompliance with data protection regulatory requirements
- Continued access to critical resources by former employees, contractors, or business partners whose access was not properly terminated
- Employees with greater access rights than necessary to do their jobs
- Segregation of duties violations due to a lack of visibility into access rights across multiple systems
- Compromised privileged accounts with extensive access rights resulting in significant access to critical data and systems

BEWARE OF THE INSIDER THREAT

While protection from outside threats is vital, securing the organization from insider threats should also be a high priority. A former employee, for example, who may have bad intentions and still have his access to internal resources can quickly do a lot of damage. In addition, an insufficiently secured cloud environment could pose a significant threat, with employees increasingly working in a digitalized world outside the four walls of the office.

Protecting critical assets against insider threats is a balancing act between locking down systems so employees and other insiders cannot get access to information outside of their remit, while allowing users sufficient access so that they can do their jobs unhindered.

Implementing a robust IGA solution combined with rigorous enforcement of policies and procedures will ensure that business operations are able to continue without exposing the company to unnecessary risk.

SECURITY AND THE PROCESS OF GOVERNING IDENTITIES AND ACCESS

Managing user access throughout a modern IT environment can be challenging, time-consuming, and vulnerable to human error. Without the proper technologies, processes, and procedures in place, your company could expose itself to a variety of security and compliance breaches.

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 the event of a security breach occurring.

Five IGA Essentials
that improves your cybersecurity strategy

Modern IGA solutions provide real-time access control to manage employees, contractors, and external identities securely. This enables the implementation of continuous identity risk protection through conditional access and classification of data backed by a cross system access suspension workflow to effectively lock down a user's access depending on the severity of a potential security breach. Using this type of dynamic approach will ensure that an organization is able to rely on the implemented policies and rest assured that they comply with relevant industry standards and regulatory authorities, while still providing the correct access, to the correct user, at the correct time. We have identified five key areas that will strengthen your cybersecurity strategy and will be describing each in more detail on the following pages.

1. IDENTITY LIFECYCLE MANAGEMENT

Support your cyber security policies by ensuring employees and contractors have the right access to systems and applications, and that any access is terminated when they leave the organization. Granting access to resources according to defined roles, rules, and policies and the ability to efficiently terminate access across on-premises and cloud-based systems and applications is an essential step in securing your organization.

2. DATA CLASSIFICATION

Identify and classify the data and information held in different systems, so data can be managed in accordance with appropriate levels of security and compliance. Sensitive data or critical business information can be tagged, so it can be managed accordingly and any access to sensitive data can be monitored efficiently. The tags allow organizations to establish a risk management strategy and apply appropriate risk controls where relevant.

3. GOVERN PRIVILEGED ACCOUNTS

Having visibility and control of privileged access rights across all business systems throughout an organization is key to ensuring security and compliance. IGA governance processes provide a fine-grained access overview to allow organizations to monitor privileged access rights. and determine who has access, why, and for how long, who approved it, and set validity periods, to ensure access is revoked automatically when no longer needed.

4. SECURITY BREACH MANAGEMENT

In the event of an incident where an organization suspects a security breach, the IT security team may want to suspend access to one or more identities immediately to prevent the lateral spreading of the breach. Identity security breach processes provide an emergency lockout option which enables an administrator to disable a user's access to all on-premises and cloud-based systems. Cross-system access suspension limits exposure to further breaches while an investigation is carried out and the user's passwords are reset.

5. RECONCILIATION / REMEDIATION

To ensure that the desired levels of security and compliance required by the organization are in place and maintained, it is necessary to continuously check that the desired security and compliance state matches the actual access state across systems and applications. In case of a mismatch, the differences need to be rectified to maintain the appropriate security and compliance levels. Reconciliation provides what security practitioners are looking for, allowing them to be confident that security issues are detected and remediated reliably.

1. Identity Lifecycle Management
Secure your Infrastructure

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 security policies to ensure employees have the right access levels at any given point in time.

ENABLE THE BUSINESS WITH SECURE ACCESS

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 life including name changes, temporary maternity leave, leaving and rejoining the organization, and more.

The removal of any access to systems that an employee used in their previous job role, but no longer requires in the new role, ensures that 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.

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 requests, and governance reporting.

EXTEND YOUR 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 does not just focus on employees, since the actual environment is often more complex. Companies typically also need to manage third parties such as contractors, seasonal workers or business partners, who need access to company resources to work efficiently. 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.

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.

2. Data Classification
Identify Your Critical Data

Use IGA to improve your cyber defense by identifying your mission critical data, and ensure you have on-demand visibility and control of exactly who can see what data.

CONTROL ACCESS TO MISSION CRITICAL DATA

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 means that they can easily be identified when specific company processes need to be applied.

Classification tags and classification tag categories (groups of classification tags) are added to object types to help organizations enforce security and comply with company policies and government data regulations. Data classification tag categories should be defined to match the type of business and national context that the organization operates in.

IGA processes allow the data administrators to create classification tag categories - for example, the 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.

SUPPORT RISK MANAGEMENT

Support the risk management strategy and enforce security policies by taking advantage of classification tags and surveys to identify critical and sensitive data. The tags allow organizations to establish a risk management strategy and put relevant risk controls in place.

When classification tag categories and classification tags have been set up, data objects are tagged using surveys - classification survey, resources classification survey, or system classification survey – depending on what is to be classified. These classification 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.

3. Govern Privileged Accounts
Ensure Continuous Control

Few users need administrative rights with wide-spread access, and therefore such privileged accounts should be removed wherever possible. Domain administrator rights for system administrators should also be limited and allocated for a limited time only. If it is easy for a system administrator to move around in a system, it is easy for an attacker to do the same.

ADMINISTRATOR ACCESS - A PRIZED POSSESSION

Administrator access to on-premises application servers, cloud-based CRM, or ERP applications, or other business critical systems is a prized possession for both internal and external attackers wanting to breach an organization's cybersecurity defenses. Compromise of privileged accounts allows criminals to probe multiple systems for confidential business data for extended periods of time.

Compromised privileged accounts not only give attackers access to a broad range of an organization's data but also allow them to potentially go undetected for months as it is not considered suspicious for administrator accounts to access all areas of the business. As a result, it is critical to ensure that administrator accounts with significant levels of access to business systems are tightly controlled on an ongoing basis so that employees and contractors only have access to the resources they need to administer and no more.

To prevent breaches involving the use of privileged accounts, organizations first need to understand which employees already have administrator access. Once this has been established, these access permissions should be verified, and any unnecessary rights revoked. After gaining control of the privileged accounts, it is necessary for the organization to put governance policies and procedures in place to manage the ongoing granting and revoking of access rights to critical business services.

VISIBILITY AND PROACTIVE RISK CONTROL

Having visibility and control of privileged access rights across all business systems throughout an organization is key to ensuring security and compliance. Identity governance processes provide a fine-grained access overview to allow organizations to monitor privileged access rights. and determine who has access, why, for how long, who approved it, and to set validity periods, to ensure access is revoked when no longer needed.

Adding identity lifecycle management and identity governance processes to the privileged accounts gives organizations the power to centrally control such accounts and their entitlements to ensure a high degree of security:

- Manage and gain visibility into entitlements and access permissions
- Automate the granting of privileged access rights based on organizational roles and the ongoing validation of all user entitlements
- Grant temporary privileged access for contractors, members of projects or employees working on time-bound assignments
- Manage segregation of duty policies across standard and privileged accounts to maintain least privileged principles
- Demonstrate compliance and accountability for authorities via advanced reporting and analytics options

4. Security Breach Management
Be Prepared

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.

LIMIT BREACH EXPOSURE

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.

IGA provides automated identity security breach processes to perform emergency lockouts which enable the administrator to instantly disable a user's access to all on-premises and cloud-based systems.

Cross-system access suspension limits the organizations exposure to further breaches while an investigation is carried out and the user's passwords are reset. An emergency lockout procedure can be triggered using an automated 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.

Identity Security Breach processes:

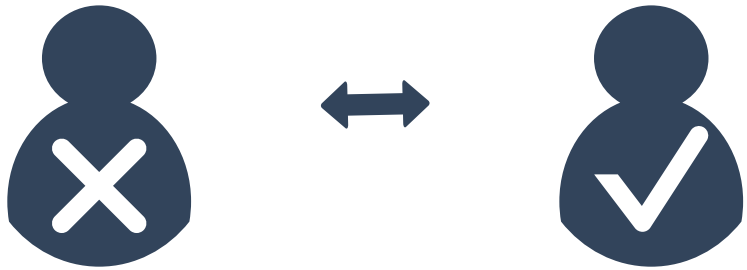
1. Give administrators the ability to suspend all accounts associated with an identity
2. Allow the administrator to reactivate the access once the situation is under control

STOP AN ATTACK

The emergency lockout quickly stops the 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 notifications management, thus protecting the company's reputation and brand.

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 may continue as before.



5. Reconciliation
Compare, Align, and Take Action

Use reconciliation to check access data deviations, uncover risks, and be able to take immediate action. Automated processes for the comparison and alignment of actual access data in IT systems with the desired permissions, also known as reconciliation, is an essential aspect of IGA and cybersecurity.

TIGHT, PERMANENT CONTROL OF ACCESS RIGHTS

Reconciliation allows the organization's security team to keep a tight, permanent control of access rights after successful access provisioning. Without reconciliation there is no real access governance. Additionally, reconciliation facilitates the operation of identity management and access governance.

The basis of reconciliation is to collect and capture the actual accounts and access rights data from all connected systems and match these up with the desired state according to business policies, SoD rules, contexts and roles. An IGA solution compares the two states and detects any differences. Mismatches between the actual and desired states are a clear compliance violation and the reconciliation process provides a comprehensive access overview highlighting such violations.

A "SHORT CUT" TO ISO27001

In addition to compliance reporting tools, organizations need flexible mechanisms to remediate violations of rules and policies. For example, auditors or system owners should be able to kick off attestation workflows to approve or reject the actual access rights, or to designate an owner for an orphaned account. In this way, reconciliation goes far beyond simple risk discovery.

On an operational level, reconciliation is part of the "Plan-Do-Check-Act" cycle described in ISO 27001 where the first step is to plan and define an access management concept, including access policies and request processes. Next, policies and processes are configured in the access governance solution. Then reconciliation can be used to check deviations, uncover risks, taking action by assigning account owners, removing undesired access, or confirm access.

MEASURE SECURITY IMPROVEMENTS

Aside from monitoring and removing risk, reconciliation also provides a consolidated overview of the actual access that people in the organization have. It is possible to generate a number of risk reports, which highlight data quality issues and security threats. In an iterative process, the organization can confirm the required accounts and access and remove unwanted objects. With this type of reconciliation, it is much easier to cope with the task of getting to a "managed" state, as at any point in time, the organization can measure the security improvements made, providing important key performance indicators for the governance of the organization.

MANAGING AUTHORIZATIONS IN LEGACY SYSTEMS

Reconciliation can also be used in cases where organizations want to control systems that lack proper management APIs or where organizations prefer to perform administration manually. An example is legacy applications, which do not provide APIs for managing authorizations and where authorizations requests are often handled manually in the application. For these systems any administrative error or malicious action will lead to a potential security threat. In this scenario, reconciliation can often still be applied by simply downloading existing authorizations on a regular basis, comparing desired and actual states of authorizations and detecting and removing critical situations.

DETECT AND REMEDIATE SECURITY ISSUES

Reconciliation provides what security practitioners are looking for to manage access risks, allowing them to be confident that security issues are detected and remediated. The security practitioners get a key concept for a robust, modern IGA system fully aligned with compliance best practices.

Securing
The Hybrid Platform

MANAGING ACCESS ACROSS THE HYBRID PLATFORM

The digital transformation that took place in 2020 has forced many companies to move to the cloud at a faster pace than many had originally planned for. Still, most companies also have infrastructure and software in-house and have to manage a hybrid platform with a mix of applications in the cloud and on-premises.
The advantages are clear. By purchasing the functions rather than the actual equipment needed, companies are able to scale or change workloads instantly without spending money on facilities, maintenance, and, to a large degree, support.

In addition, by purchasing software, infrastructure, and platforms as-a-service rather than as boxed products, companies are also able to move the cost of all those things from capital expense to operating expense.

By moving data to the cloud, access to it becomes less a matter of location, and more of function. That means collaboration can be worldwide for even the smallest companies.

But what does the move to the cloud mean for IT departments when it comes to security? It means they need to keep greater control and overview of who has access to IT services across all assets. Without adequate overview and control, the result could be a complex, ungoverned, IT “wild west” across a variety of cloud and on-premises applications. To maintain security, the IT department must manage both on-premises applications as well as cloud-based applications and data in line with corporate policies and regulatory requirements.

WHAT YOU NEED FOR IGA IN THE CLOUD

As your operations migrate to the cloud, keeping track of governance, identities, and access issues can become more complex than ever, unless you manage them with a solution designed for hybrid environments.

To ensure security across both on-premises and cloud-based systems each of the following elements must be included in your program:

- A business process layer to automate and unify compliant access governance processes across target systems and applications
- Secure sharing of resources and cloud services with employees and business partners through automated access governance processes across cloud and on-premises applications
- A 360-degree overview and audit trail of cross-system access, accountability, ownership, and security for ensuring regulatory access compliance
- Automated identity lifecycle processes for on-boarding, off-boarding, and departmental changes for employees, business partners, and customers, to ensure access can be securely granted and terminated
- Automated role changes to ensure appropriate access as the role of an employee or partner changes, so access rights automatically change accordingly and are limited to the requirements of the current role
- Minimized risk of unauthorized access by disabling access rights for terminated contractors, partners, guest accounts or customers easily done from one central location

IGA Cyberssecurity
Next Step

Managing user access throughout the modern IT environment can be challenging, time-consuming, and vulnerable to human error. Without the proper technologies, processes, and procedures in place, your company could expose itself to a variety of security and compliance risks.

SUPPORT YOUR CYBER DEFENSE

As more and more business processes fall under the remit of IT, the importance of cybersecurity infrastructure increases. Identity management and access governance (IGA) is at the heart of the cybersecurity policy, protecting IP, sensitive data, and helping to achieve regulatory compliance as a key part of every organization's IGA roadmap for their digital future.

In addition to the five IGA essentials described in this e-book, IGA provides a wide variety of functionalities to support your cyber defense, some examples are:

- **Policy management:** Enables organizations to quickly and easily assign a set of access rights to users who meet a set of criteria and create and manage access constraint policies
- **Segregation of duty:** Automatically detects the granting of any toxic access combinations to prevent end users from being able to carry out fraudulent activities based on their access to the business systems
- **Password management:** Enables organizations to manage password policies for each business system as well as enabling users to securely reset their own passwords
- **Manage guest accounts:** Allows organizations to establish governance processes for guest accounts in Active Directory

THE RIGHT ACCESS FOR THE RIGHT PEOPLE

As your digital operations migrate to the cloud, keeping track of governance, identities, and access issues can become more complex than ever. Omada's identity management and access governance solution enables businesses to share resources and assets with employees and business partners securely and efficiently. It applies governance and control processes that secure a 360-degree overview of access, accountability, ownership, auditability, security, and access compliance.

GET STARTED

To help you kick-start the process, Omada has addressed many of the identity management and access governance challenges by creating the best practice IGA framework - IdentityPROCESS+ that gives organizations a roadmap for quickly and effectively putting standardized policies and procedures in place that manage the security and compliance of user identities. After 20 years of experience working with IGA, we can help guide you forward with proven steps that will add value to your business.

IGA
Glossary

Access management
Process 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
Process 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
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 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 six process areas: Identity Lifecycle Management, Access Management, Business Alignment, Identity Security Breach, Governance, and Administration.

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 account 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.

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, simultaneously improves 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.

omadaidentity.com