Omada Identity Cloud

Identity Governance
Software-as-a-Service

Omada

Do more with identity

www.omadaidentity.com | info@omadaidentity.com

Table of contents

Omada Identity Cloud

Enterprise-Grade IGA Software-as-a-Service

THE NEXT GENERATION OF IGA SOLUTIONS

Ensuring secure, compliant, and efficient access to critical data for key employees and partners has never been more important. Investing in reliable Identity, Governance and Administration (IGA) solutions has therefore become a top priority. But, implementing IGA requires more than just software. It requires a transformation of business processes and workflows based on the latest IGA best practices and it requires software that can be adapted to the existing IT environment.

Omada Identity Cloud provides a next generation solution that includes guidance in IGA best practices and implementation supported by enterprise-grade Software-as-a-Service (SaaS) that can be adapted to your unique organizational processes, rules, and workflows.

ENTERPRISE-GRADE IGA

Omada's award winning identity solution provides an enterprise-grade, mature Software-as-a-Service offering with a comprehensive set of IGA features. This means customers no longer need to compromise when moving their IGA implementation to the cloud but can be confident that the same enterprise-grade security and IGA capabilities are available.

The solution is fully configurable enabling support of specific requirements as well as legacy systems and interfaces without the need for custom code development. This ensures backward compatibility and a seamless upgrade path for ease of maintenance and operation.

SUPPORTING EVOLVING REQUIREMENTS

The security and governance landscape has changed dramatically over the last few years with more changes to come. IGA is the first line of defense requiring a structured, reliable, but also adaptable solution. Omada Identity Cloud is regularly updated with new features to support shifting security and governance requirements.

As a cloud-based solution, new features are available to customers immediately with no need for coordinated company-wide software updates. Powered by Microsoft Azure Cloud, the platform can scale to meet any requirement taking advantage of security, business continuity capabilities and data residency requirements.

Tangible Business Benefits

- Accelerate implementation of IGA best practice processes
- Secure access to sensitive data and resources enterprise-wide
- Identify and mitigate risks with full transparency
- Act quickly on violations with built-in automated workflows
- Master governance and compliance with automated processes and reports
- Increase productivity and satisfaction via automated control and self-service
- Significantly reduce time used by valuable and scarce human resources
- Use automated IGA processes as enabler for broader digital transformation

A Complete Solution
for Successful IGA Projects

The Omada Identity Cloud IGA platform is one of the four fundamental building blocks in the Omada IGA value proposition.
Each block plays an important part in helping customers and partners achieve excellence in managing technology, people, and processes.

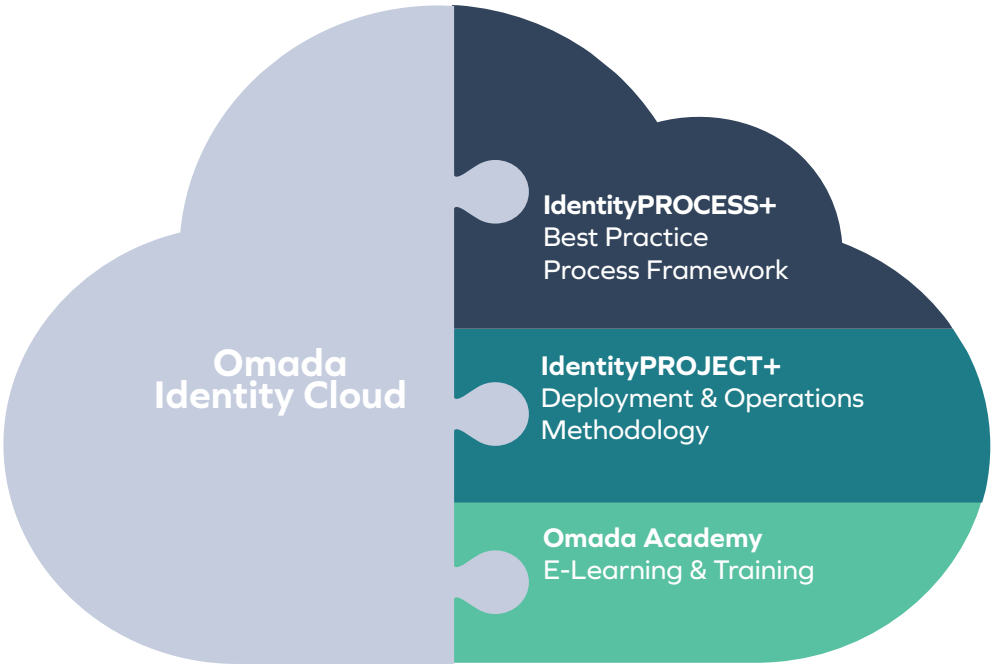


Fig. 1: Omada's four IGA building blocks

OMADA'S FOUR IGA BUILDING BLOCKS:

- **Omada Identity Cloud:** IGA as-a-Service or on-premises software installation with feature parity
- **Omada Academy:** IGA e-learning and in-person courses for partners and customers
- **IdentityPROCESS+:** The leading IGA best practice process framework
- **IdentityPROJECT+:** The proven project methodology for IGA success

These four building blocks reflect our focus on not only providing leading technology, but on ensuring the success of our customers and partners with their IGA initiatives. Together, they ensure a structured and reliable approach to IGA planning and implementation, but with the flexibility to rapidly adapt and meet new requirements with Omada's enterprise-grade IGA software-as-a-service.

Omada Identity Cloud

Identity Governance Software-as-a-Service

OMADA IDENTITY CLOUD

Omada Identity Cloud provides a mature and reliable solution for automation of IGA processes and policy enforcement. Omada Identity Cloud is positioned as a leader in the latest Gartner Magic Quadrant for IGA providing the only solution on the market with full feature parity for both on-premises and software-as-a-service offerings. This enables and supports enterprise hybrid strategies as more workloads are moved to the cloud.

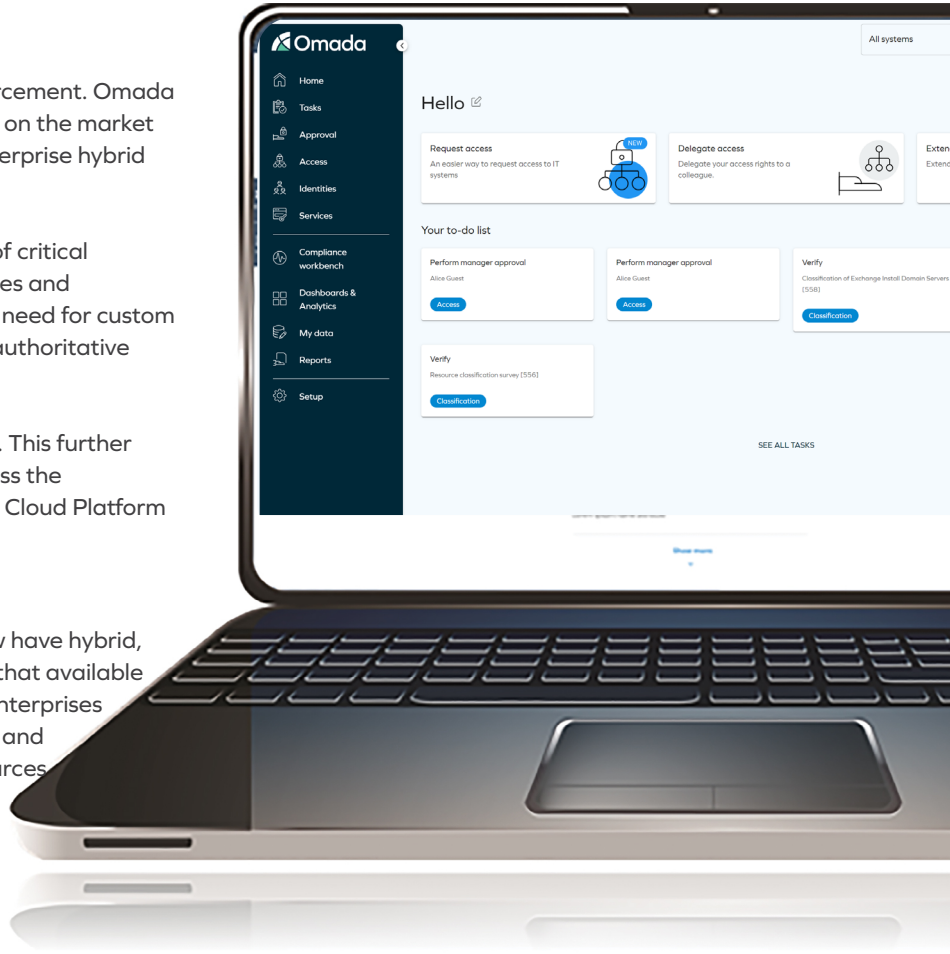
The Identity Cloud solution is designed to be highly configurable eliminating the need for custom development of critical functionality saving time, effort, and cost during deployment. A comprehensive set of best practice IGA processes and workflows are supported out-of-the-box and can be adapted to individual enterprise requirements without the need for custom development. A unique integration model enables configurable connection to other applications, systems and authoritative sources and easy integration into IGA processes and workflows.

With Identity Cloud Software-as-a-Service, all of these capabilities are available in a cloud-architected solution. This further reduces deployment time and cost eliminating the need for software installation and version management across the organization. As new capabilities, features and best practice process support are added to the Omada Identity Cloud Platform platform, they are immediately available to the entire organization.

EASE OF ADOPTION, INTEGRATION, AND OPERATION

Omada Identity Cloud is designed for the real world. The flexible solution design addresses that enterprises now have hybrid, heterogeneous environments based on the latest cloud solutions, but also critical legacy systems. It recognizes that available data is imperfect and that preparing data for IGA processes is a major undertaking. It recognizes that no two enterprises are the same and that processes and workflows need to be adapted so that it is the tool that fits the enterprise and not the enterprise that needs to adapt to the tool. It recognizes that enterprises do not have the time and resources to provide or consume custom code development.

Identity Cloud is therefore designed to ease the adoption, integration, and operation of the latest best practice IGA processes across the modern heterogeneous enterprise environment. It is designed to be fully configurable through intuitive web-based interfaces including data models, objects, and attributes. It provides standard processes, workflows and connectors to hundreds of applications, systems, and authoritative sources out-of-the-box, all of which are configurable. This accelerates the implementation of IGA processes with a solution that fits your unique environment.



ENTERPRISE-GRADE IGA

The term "enterprise-grade" is often used, but not often understood. In the context of IGA, enterprise-grade refers to the complexity of modern enterprise IT environments and the need for solutions that make managing and governing that environment easy.

Enterprises now rely on a host of applications and systems both installed on-premises and in the cloud, some of which are centrally controlled and some which are controlled by individual departments and groups. Providing a unified approach to IGA requires solutions and platforms that can span this heterogeneous environment, understand the context, and enable automated control and governance.

Omada Identity Cloud is an enterprise-grade IGA SaaS solution that provides the critical functionality modern enterprises need to stay ahead of developments. The functionality provided by Identity Cloud is designed to support the explore, build and operate phases of the Omada IdentityPROJECT+ implementation methodology with out-of-the-box support for best practice IGA processes as described in the Omada IdentityPROCESS+ framework.

The combination of enterprise-grade functionality supporting a well-defined methodology and out-of-the-box process support makes Omada Identity Cloud the most comprehensive IGA solution on the market today.

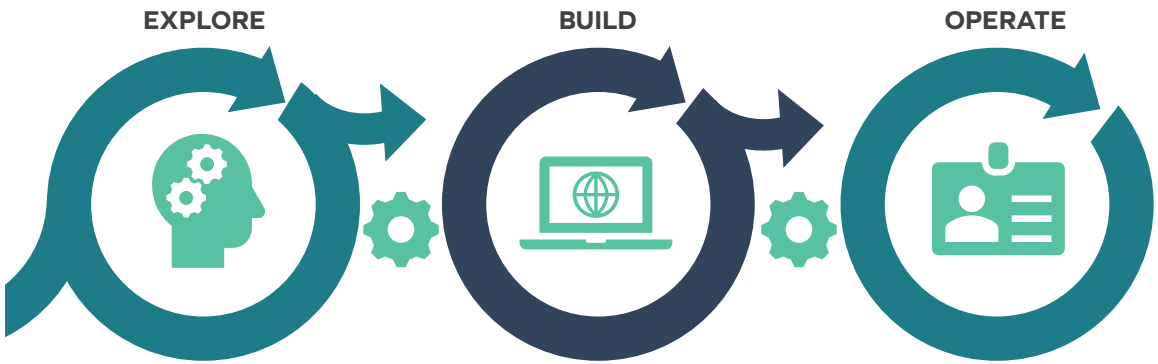


Fig. 2: The three IdentityPROJECT+ phases

"Omada has one of the most robust auditing mechanisms among the IGA players, with out-of-the-box case management capabilities to react to violations and other audit events, including formal case handling workflows to manage incidents into closure."

[Source: Leading Analyst Company]

Enterprise-Grade IGA
Processes and Functionality

FUNCTIONAL AREAS
Data Cleaning, Workflows, and Applications Integration

Data Cleaning

- Establish a consolidated data model
- Data matching using fuzzy logic
- Data de-duplication
- Automatically enrich and modify data objects with data classification policies
- Simultaneous matching of multiple authoritative sources
- Prioritization rules for identification of primary identity source
- Data matching validation processes

Configurable Workflow Engine

- Comprehensive best practice IGA process framework
- Option for manual, triggered, or scheduled workflows
- Pre-configured email integration and email prompts
- Configuration of workflows, processes, and forms via web-based interface
- Activity assignment based on policies and rules
- Configurable escalation process

Application Integration

- Integration model for application, system and authoritative source connection
- Extensive range of standard connectors
- Authoritative sources such as SAP HCM, SuccessFactors, Workday, UltiPro
- Integration with ITSM, SIEM, PAM, Data Access Governance
- Open extensible platform with SDKs and APIs
- Authentication via OpenID Connect and SAML

FUNCTIONAL AREAS
Access Roles and Privileges

Role Lifecycle Management

- Management of role lifecycle processes, role mining and modelling
- Role mining tool for analyzing and building roles based on data from connected systems
- Mining based on identity types, identity templates, identity attributes and identity relations

Access Process Automation

- Multiple policy types for automation and control of access processes
- Automated assignment of access based on organizational policies
- Constraint policies for determining access eligibility
- Segregation of Duty (SoD) policies and constraints
- Dynamic organizational modelling
- Extendable role and policy engine
- Intelligent control policies with automated case handling workflows

FUNCTIONAL AREAS
Managing Identities and Access

Identity Lifecycle Management

- Control access rights to data, applications and resources according to defined assignment policies
- On-boarding of employees and contractors
- Access based on role or context and automatic revocation upon changes to that role or context
- Sourcing of identity data from multiple authoritative data repositories
- Act as authoritative source

Automated and Unified Provisioning

- Unified provisioning to heterogeneous IT systems
- Choice of automated, partly automated or fully manual provisioning
- Integration with service desk solutions

Self-Service Access Request

- Portal for users and managers to request access to data and resources
- Context-based self-service access request
- Multi-level configurable approval workflows
- Serial and parallel approvals
- In-process SoD policy checks
- Requests for multiple identities, systems and resources in one request

Business Partner Enrollment

- Customer Identity Access Management (CIAM) self-service tool
- Allow partners and customers to register for access to relevant information
- Web-based login or log-in based on social media accounts

Password Management

- Ability for users to change passwords without involving the helpdesk
- Users can reset passwords for owned accounts or on behalf of other users
- Synchronization across connected applications enabling single sign-on

FUNCTIONAL AREAS
Certification, Compliance and Risk

Cross-System Access Certification

- Validation and approval of current state of access to ensure compliance and security
- Access certification on entitlements, identities, and account ownership
- Configurable survey types for user entitlement, account, permission entitlement reviews
- Triggered based on events or scheduled for periodic re-certification
- Efficient interface for search, sorting, look-ups and forwarding for re-assignment
- Survey types compliant with strict regulatory requirements
- Central monitoring of certification campaigns
- Automated escalation and notification
- Standard certification audit reports

Compliance and Auditing

- Cross-system reporting and analytics
- Actionable dashboard for compliance-related controls
- Full compliance overview across connected systems and applications with ability to drill-down into details
- 50+ standard reports available
- Configurable KPI dashboards
- Historic reports enabling forensic analysis
- Ability to modify report types and define new report types

Risk Management

- Computation of risk scores to support approval workflows, access reviews and risk monitoring
- Risk scores computed for systems, resources, resource assignments, accounts and identities
- Risk classification tag with risk factor and risk weight
- Display of risk scores based on configurable intervals

FUNCTIONAL AREAS

Data Cleaning, Workflows, and Applications Integration

DATA CLEANING

With Omada Identity Cloud data quality does not need to be perfect when you start. Unlike other IGA solutions that require perfect data before they can be used, Omada Identity Cloud is built to accommodate real-world situations. Data is often required from disparate sources with their own data models and needs to be processed before a reliable consolidated data model can be established. Omada Identity Cloud provides a robust process for data matching, enriching, and cleaning during application onboarding.

Control policies automatically check for master data and entitlement data quality issues, including 'missing manager information', replacing resource owners that are no longer employed, handling of duplicate identities and other validity issues. Omada Identity Cloud data cleaning functionality establishes control and continued assurance of data quality for IGA processes.

CONFIGURABLE WORKFLOWS

Omada Identity Cloud supports a comprehensive range of IGA best practice processes and workflows out-of-the-box. These can be configured to meet your specific needs without the need for costly and time-consuming programming effort. This includes the ability to add new workflows and processes as well as configure escalation concepts. Activities can be assigned and reassigned to users or user groups based on automated calculations, policies, and rules.

This is made possible by a dynamic workflow and process engine that is configurable and extendable. The engine is configured through an intuitive web-based interface without the need for custom code. Workflows can be configured to be manually launched, triggered by events or scheduled. Workflow reminder services and email integration are provided out of the box.

APPLICATION INTEGRATION

Omada Identity Cloud provides a unique integration model to easily connect to relevant applications, systems, and authoritative sources. This includes integrating applications and systems into existing role concepts and access management processes. A wizard supports easy configuration of the attributes of the application or system, such as definitions, data mappings, data import and provisioning methods. Built-in dashboards provide an intuitive overview of the systems, ownership, risk classifications and more. Omada Identity Cloud ensures enterprise-wide access control of all relevant applications, systems, and data.

Omada Identity Cloud provides hundreds of standard connectors for on-premises and cloud-based solutions. In addition, it provides an open extensible platform with accessible SDKs and APIs as well as authentication via OpenID Connect and SAML.

> "Omada's product offers a robust process for cleanup during application onboarding."
>
> [Source: Leading Analyst Company]

FUNCTIONAL AREAS

Access Roles and Privileges

ROLE LIFECYCLE MANAGEMENT

Establishing explicit roles with defined privileges is critical for ensuring that only the right people can access the right data at the right time. The Omada Identity Cloud role mining tool supports the analysis and establishment of enterprise-wide roles and privileges. Role Mining is performed on live production entitlement data extracted from connected applications, systems and authoritative sources. The tool is capable of determining the roles that provide the best fit to the organizational hierarchy by traversing the organizational structure and establishing policies for organizational level privileges.

Role Mining can be based on parameters such as identity types (e.g. employees, consultants, business partners, customers etc.), identity templates (e.g. selected employees, business functions, business roles), identity relations to organization and placement in the organizational hierarchy (OU's) and identity attributes (e.g. job function, location etc.).

ACCESS PROCESS AUTOMATION

Omada Identity Cloud provides a range of powerful policy types out-of-the-box, which enables full automation of access processes. These include assignment policies, constraint policies, control policies and Segregation of Duty (SoD) policies. Each policy plays an important role in ensuring security, compliance and efficiency. Assignment policies ensure that access privileges are aligned with organizational policies while constraint policies control which data and resources roles are eligible to access. SoD policies address the real-world issue of conflicts in access rights due to an individual having multiple roles and ensuring that "least access" privilege practices are enforced. Intelligent control policies include automated case handling workflows that automate the response to audit events and access violations saving time when responding to what could be serious events.

These policies and constraints are critical, as security breaches regularly exploit discrepancies in access rights. They are also essential in ensuring compliance with strict governance procedures and industry standards.

Omada Identity Cloud enables enterprise-wide policies and controls to be established with automated enforcement. Dynamic organizational modeling supports automated assignment of access rights based on organizational policies. An extendable role and policy engine enables continuous refinement of access policies. These capabilities eliminate the need for human intervention increasing organizational efficiency.

> "Omada's product has a very flexible risk scoring system."
>
> [Source: Leading Analyst Company]

Assignment of Resources
Based on Policies

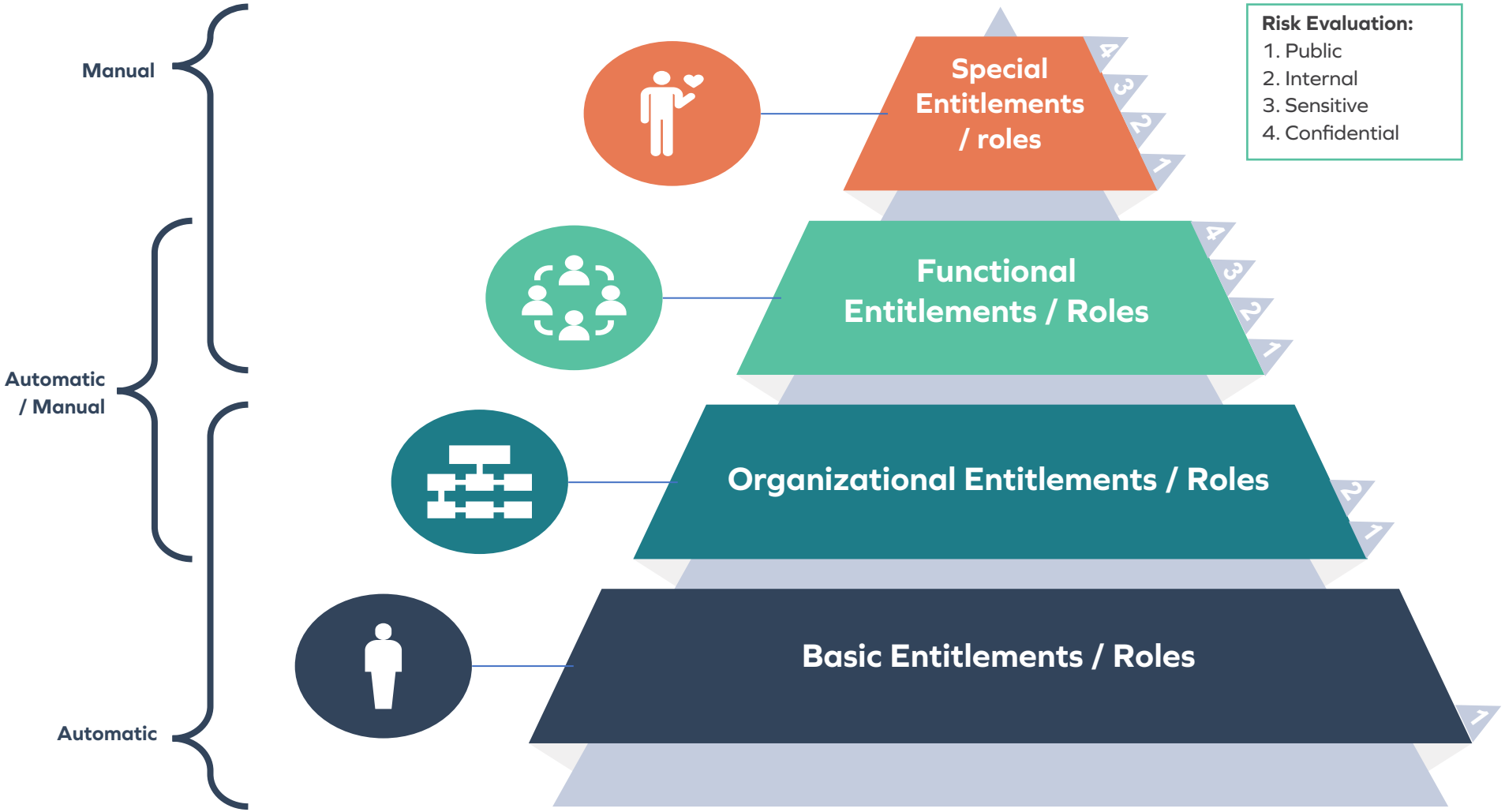


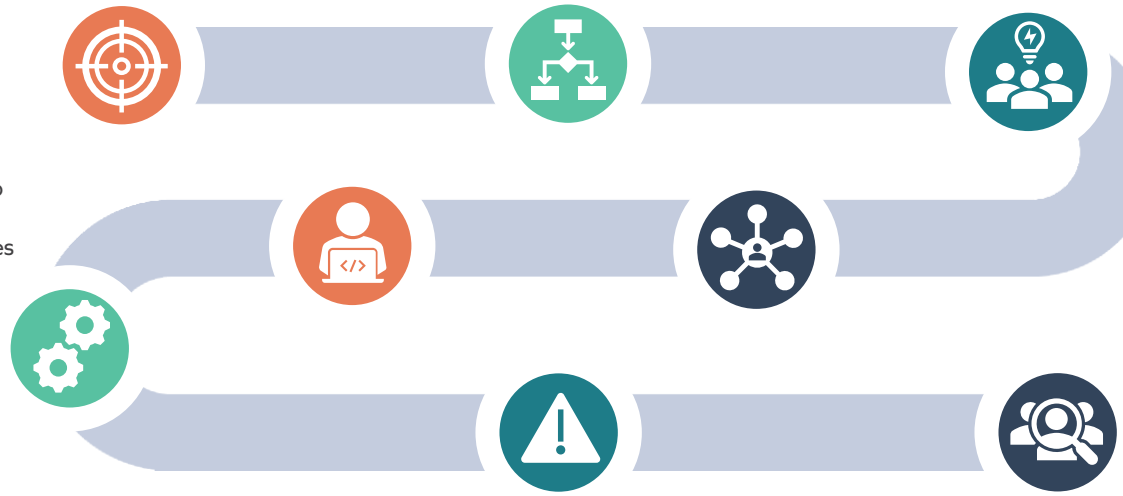
Figure 3: Omada provides a concept for modelling, defining, mining, and maintaining and enterprise-wide role model.

Governing the Lifecycle of Roles and Privileges

1. General objectives
- Compliance and/or efficiency goals
- Verification of role modeling method
- Project scope: Applications, identities, context

2. Define role model
- Role Model Principles
- Role types
- Model hierarchy
- Critical Use Cases (e.g. request and approval scenarios)

3. Verify the role model
- Stakeholder identification: application owners, master data owners, administrators, IT auditors, IT security etc.
- Get buy-in through work-shops with key stakeholders



4. Design role management processes
- Create (new role)
- Change / Revision
- Delete
- Evaluate role quality

5. Produce roles
- Mining and designing
- Top-down meets bottom-up
- Validation of roles
- Potential assignment policies
- Consequence analysis

6. Integrate roles in access management processes
- Business descriptions
- Requests and approvals
- Risk mitigation

7. Establish risk concept
- Regulations
- Data protection
- Risk classification
- Segregation of duties (SoD)

8. Role audit processes
- Recertification
- Role model quality, e.g. overlapping roles
- Role quality
- Compliance dispensation

FUNCTIONAL AREAS

Managing Identities and Access

IDENTITY LIFECYCLE MANAGEMENT

Advanced Identity Lifecycle Management enables control of individual access rights to data, applications, and other types of resources according to defined assignment policies. This supports processes for on-boarding and off-boarding of employees and contractors, as well as revocation of access to resources as an individual or organization's role changes.

This includes key events in the identity's lifecycle, such as a contractor being converted to an employee, delegation of responsibilities or parental leave. Identity data can be sourced directly from one or more authoritative data repositories, such as HR systems or the platform itself can be an authoritative source for others, such as contractors.

AUTOMATED AND UNIFIED PROVISIONING

Implementing IGA processes requires provisioning across all connected systems, applications and authoritative sources. Omada Identity Cloud provides multiple, flexible provisioning options across the heterogeneous enterprise environment. This enables provisioning with assignment policies to be fully automated. For some environments, full automation is not possible.

Omada Identity Cloud therefore provides the option of defining that parts or all of the provisioning process are performed manually. Omada Identity Cloud can also be integrated with a service desk solution to fully support the provisioning process. This includes relayed provisioning functionality that allows the creation of a work item inside an IT service management tool.

Automation and management of the complete identity lifecycle

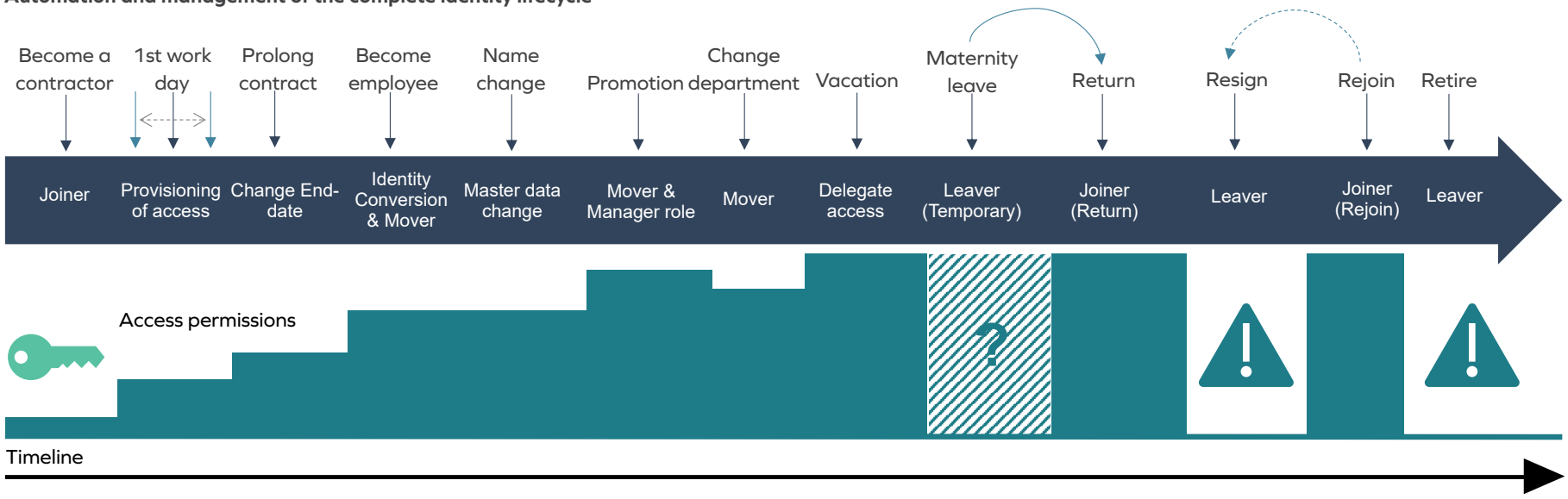


Figure 4: The platform supports the complete identity lifecycle management process with a comprehensive set of standard processes for identity lifecycle scenarios and automated provisioning of access permissions.

SELF-SERVICE ACCESS REQUEST

Omada Identity Cloud provides a Self-Service Access Request capability that makes it easier for users and managers to request access without the need for human intervention. Based on a user-friendly portal, it enables users to request multiple services in one request also on behalf of others, such as managers requesting access for their employees.

Delegated administration can be based on management reporting lines with serial and parallel approvals or other appropriate rules. Access can be requested within a context such as job functions or projects and Omada Identity Cloud ensures that access privileges are removed automatically as soon as the context membership is terminated, supporting the principle of "least privilege" access.

BUSINESS PARTNER ENROLLMENT

Omada Identity Cloud provides a Customer Identity Access Management Self Service (CIAM)
experience that enables customers and partners to register for secure and fast access to relevant information.

Log-in by customers and partners is performed via a browser interface or through social media log-in functions. Identities and accounts are created automatically. CIAM significantly reduces the administrative burden of providing access to external parties while increasing the efficiency of cooperation and collaboration.

PASSWORD MANAGEMENT

Password Management processes enable users to reset their password without contacting the helpdesk. Users can reset passwords for owned auxiliary accounts, or on behalf of other users, such as allowing a manager to reset the password of a managed identity.

Passwords can be synchronized across all connected applications enabling single sign-on so the user need only remember one password thus reducing the risk of password exposure to bad actors.

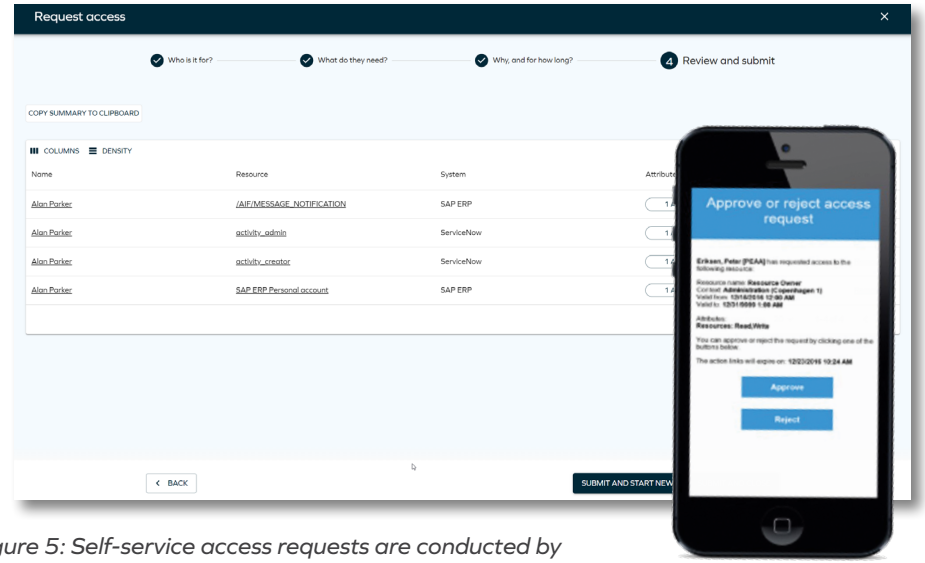


Figure 5: Self-service access requests are conducted by managers or employees in a user-friendly interface allowing users to easily request access.

Best Practice Processes

Access Request and Approvals

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. The process automates access requests enabling end users to provide the right information so that access can be granted quickly without introducing security and compliance violations. Based on defined policies the automated evaluation processes determines whether inappropriate combinations of access rights have been assigned, detects any violations, and allows managers to evaluate the situation to decide whether access should be allowed or blocked.

Omada Access Request Process

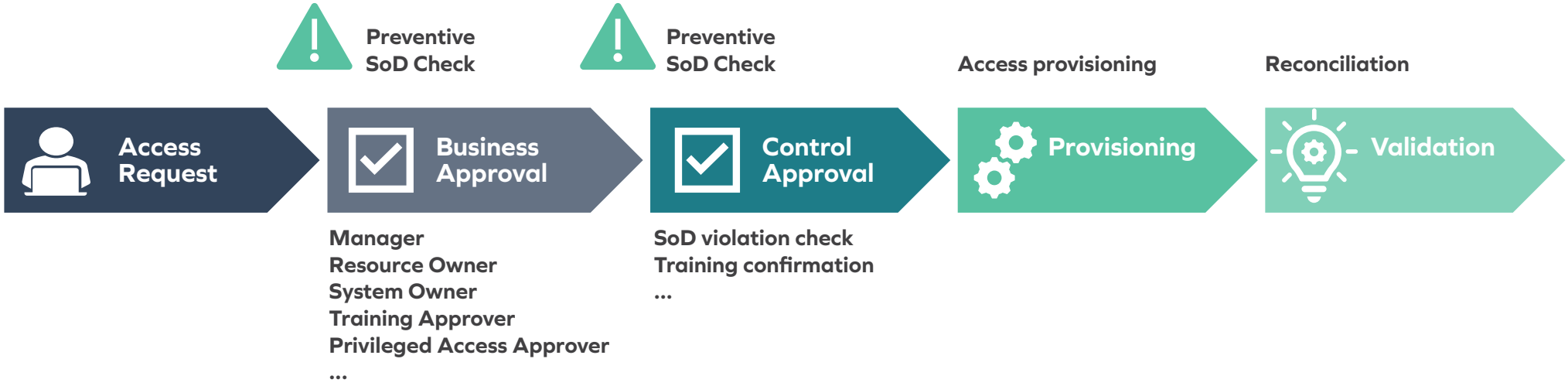


Figure 6: Best practice processes such as approval processes are provided out of the box and can be configured to meet your specific needs.

FUNCTIONAL AREAS

Certification, Risk, and Compliance

CROSS-SYSTEM ACCESS CERTIFICATION

Access certification enables the validation of the current state of access to ensure that it is compliant and secure. Access certification and re-certification can be performed on entitlements, identities, account ownership and much more.

Omada Identity Cloud features multiple configurable campaign types ("survey types") that meet best practice recommendations and strict regulatory requirements out-of-the-box. These include user entitlements reviews, accounts reviews, permission entitlements reviews, permissions reviews, periodic roles, and business description reviews. Campaigns can be centrally monitored with automated escalation and notification. They can be configured for any type of object and can be triggered based on events or scheduled for periodic re-certification.

RISK MANAGEMENT

Omada Identity Cloud provides a powerful Risk Management concept that adds value across systems, processes and controls. The risk concept can be used in the approval of workflows and to understand the severity of audit events and other notifications. Risk scores are computed for systems, resources, resource assignments, accounts, and identities.

The risk calculation of a resource is based on its classification. Each applied classification tag can carry a risk factor and a risk weight. Risk scores are displayed in user-friendly values based on configurable intervals. This supports harmonization and agreement across the organization on risks associated with access rights and events that occur.

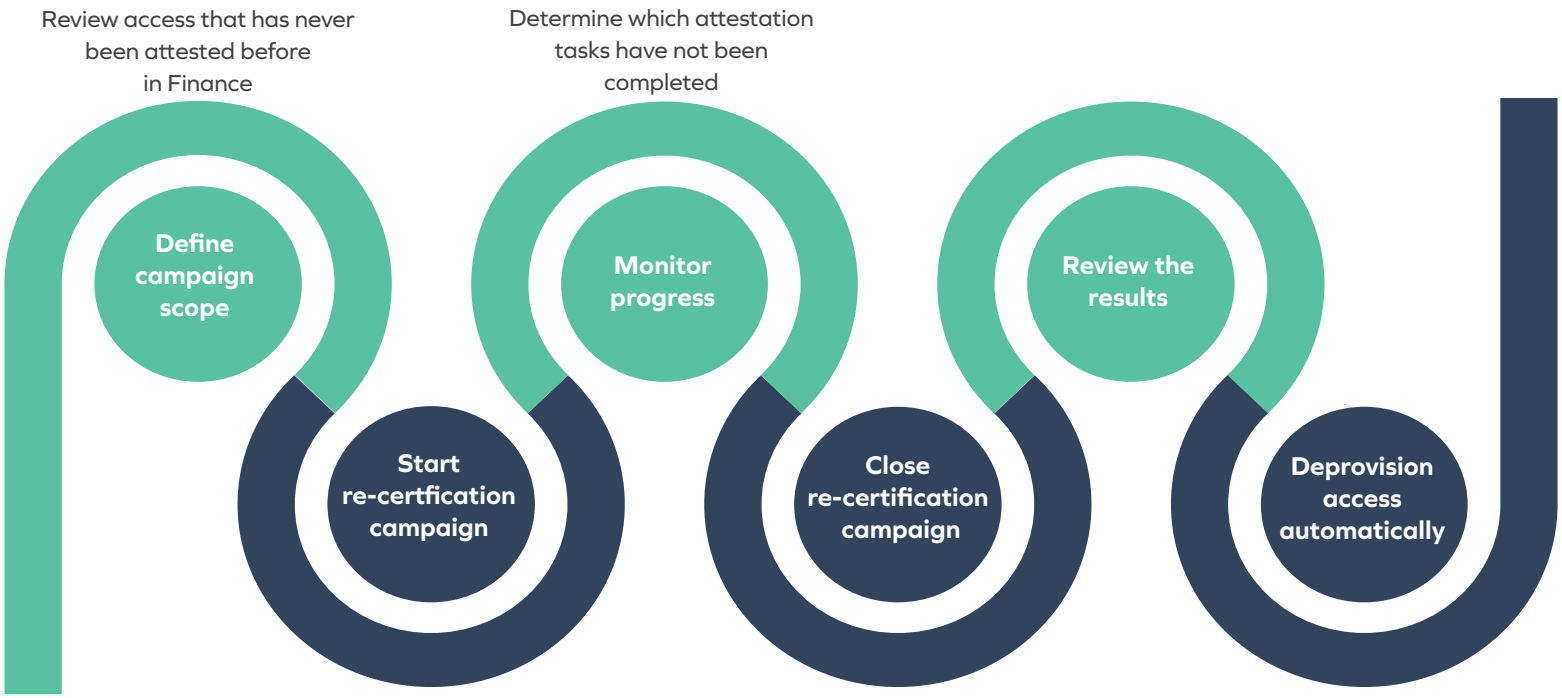


Figure 7: The platform automates the complete Access Certification cycle. Campaigns can be modified to your specific needs via configuration.

COMPLIANCE AND AUDITING

Omada Identity Cloud provides powerful compliance and auditing capabilities. Cross-system reporting is available for current and historical overviews and analysis. The built-in analysis and reporting features deliver identity intelligence and answers to the basic questions of 'who has access to what', and 'who approved the access'. For instance, it is possible to track each access request made, whether initiated by HR changes, self-service requests or via automated assignment policies, such as assignment of birth rights.

Several dashboards are included such as an actionable dashboard for compliance-related controls, such as orphaned accounts and unapproved access remediation and KPI dashboards.

Omada Identity Cloud supports continuous monitoring of compliance and supports automated, as well as manual actions and mitigations. It provides a "true" overview, which is an important audit requirement.

Reconciliation is performed by continuously calculating the delta between the state of monitored systems and the desired state. Omada Identity Cloud gathers and reconciles data from the connected applications, systems and authoritative systems enabling reporting and data analysis.

An actionable compliance dashboard provides an overview of issues making it possible to mitigate risks and inconsistencies efficiently and effectively.

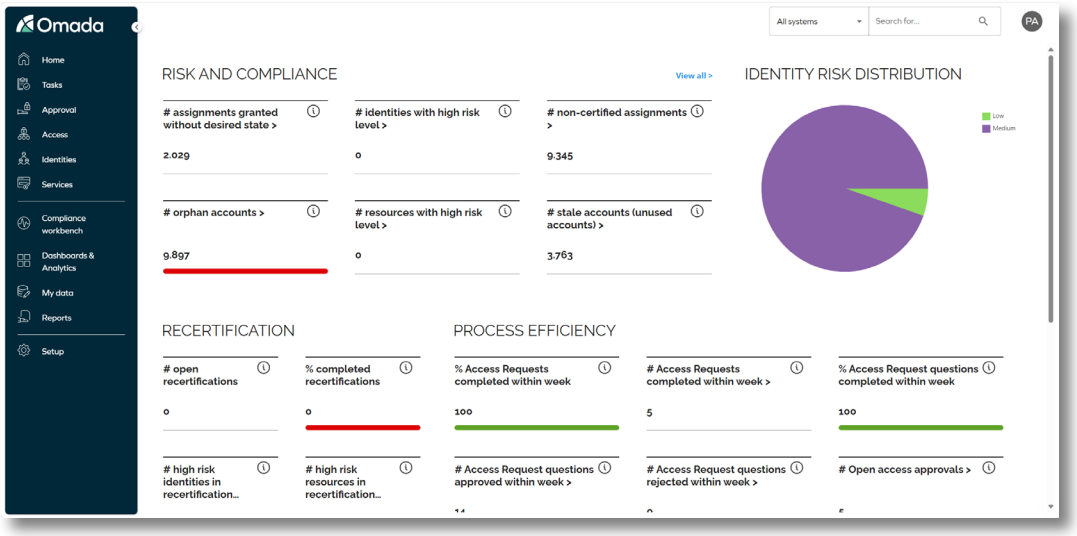


Figure 8: A configurable KPI Dashboard provides a great overview of important KPI's.

> "Omada has one of the most robust auditing mechanisms among the IGA players, with out-of-the-box case management capabilities to react to violations and other audit events, including formal case handling workflows to manage incidents into closure."
>
> [Source: Leading Analyst Company]

Systems Overview and In Depth Data Analysis

Compliance Dashboards

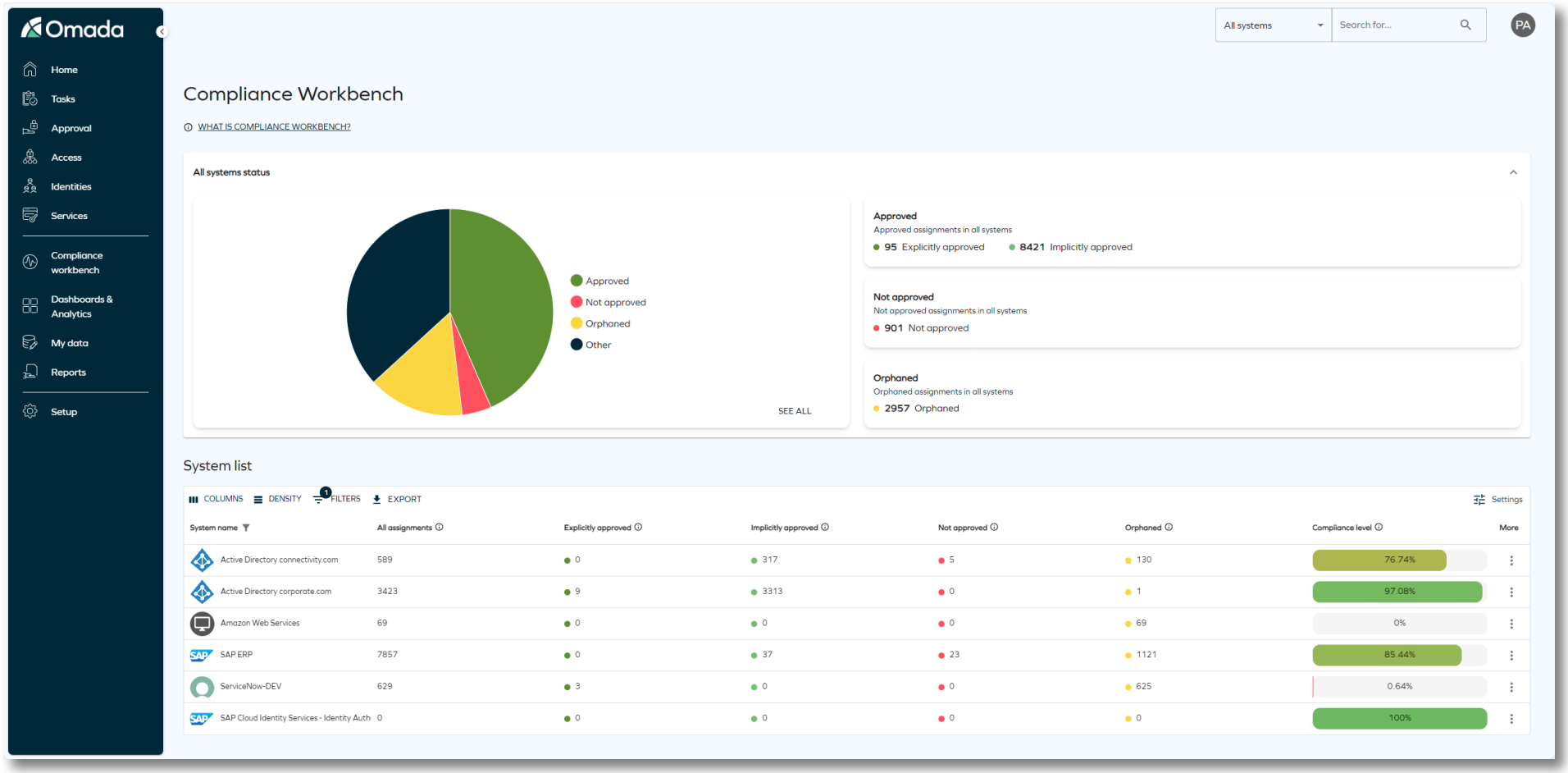
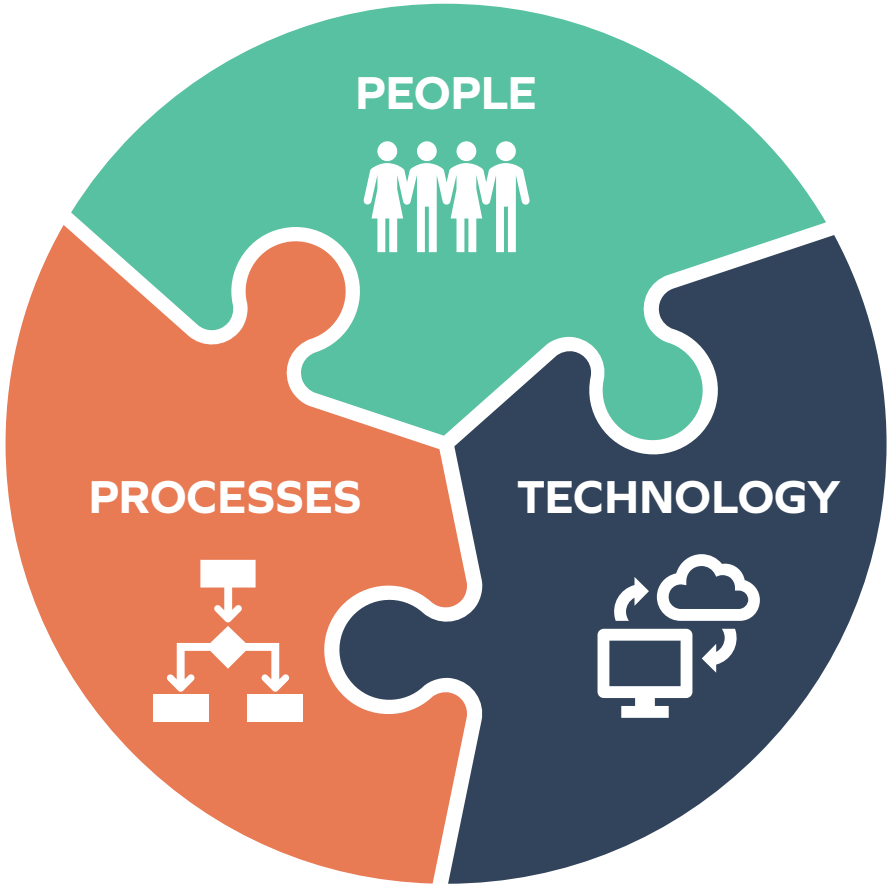


Figure 9: A Compliance Dashboard provides a valuable cross system overview providing the compliance status for all governed systems and applications. The dashboard provides the ability to drill down for in-depth detailed data analysis. Mitigating actions, workflows and certification campaigns can be launched directly from the dashboard.

Omada Identity Cloud

The Foundation for Business Transformation

Omada Identity Cloud supports the Omada IdentityPROCESS+ framework and IdentityPROJECT+ methodology and thus accelerates the implementation of IGA best practice processes in heterogeneous enterprise environments. This recognizes the need to address people and processes as well as technology if one is to succeed in implementing IGA. With a successful IGA implementation, organizations have established a foundation that can support further business transformation. Ensuring secure, compliant, and efficient access to critical data and resources accelerates business transformation initiatives with low risk and greater potential for success.At Omada, we have designed Omada Identity Cloud to ensure that the foundational process of implementing best practice IGA is the first success on your business transformation journey.



A Scalable and Secure Platform
Powered by Microsoft Azure

Omada Identity Cloud is hosted on Microsoft Azure, one of the most reliable, scalable and secure cloud hosting platforms available.

- Support for regional data privacy requirements
- Microsoft Azure provides "geo-redundancy" with database backup allowing the region where data is stored to be selected as well as backup to an additional region to ensure business continuity
- ISO certified support and operations
- Omada Identity Cloud provides the highest security standards based on both standard Azure security features as well as vulnerability and penetration testing performed regularly by Omada according to ISO 27001
- Omada is a member of the Microsoft Intelligent Security Association (MISA) supporting the sharing of threat intelligence data among identity and access management providers.

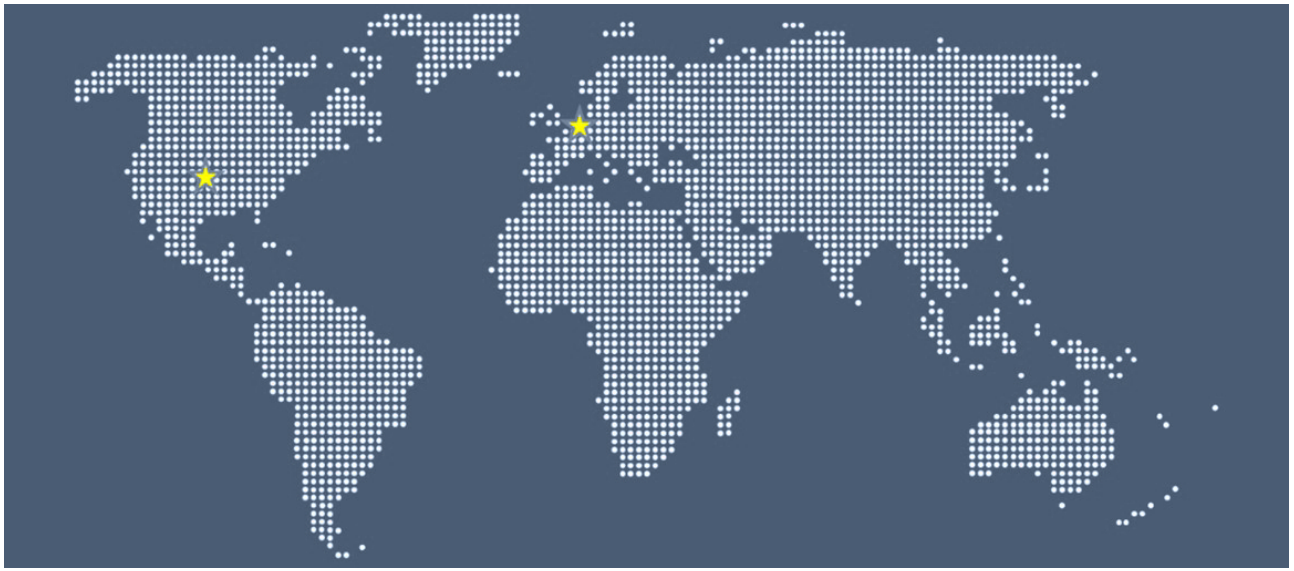


Figure 10: Omada runs on Azure and can provision in any Azure region. Azure is currently provided in 58 regions worldwide and is available in 140 countries/regions.

Omada Identity Cloud

Services Included in Subscription

Omada Identity Cloud Enterprise-Grade **IGA SaaS**

High-availability service with **99,9%** availability

Critical incident response times are guaranteed within maximum **1 hour**

Critical incident updates every **30 minutes**

24/7/365 service support covering 2nd and 3rd level support

Tiered **deployment environment** included for Non-Production and Production

Unlimited number of **connected** systems

Unlimited **data storage** and unlimited traffic

Flexible **upgrade** windows that fit your business needs

Service **continuity** management

Disaster **recovery and backup** services

Continuous reporting, **health check** and log handling

Ongoing **automated deployment** of releases and patches

Access to **Omada Service Desk**

Access to Omada knowledge sharing **HUB**

OMADA SERVICE DESK SUPPORTS YOU WHEN YOU NEED IT!

The Omada Service Desk is your customer-centric entry point for any incidents, service requests and feature requests. Our Service Desk is staffed with skilled support engineers and service delivery managers who are there to serve you and who handle any incoming requests from your organization with constant care.

Our team ensures that you receive timely progress notifications. Access to the ITSM-system is also provided allowing the latest status of your ticket to be viewed at any time. Reports on agreed Key Performance Indicators (KPIs) are provided regularly to ensures constant improvement in efficiency and an optimal customer experience.

The service subscription includes a four-tier escalation process providing a means for customers to escalate the ticket and ensure timely resolution.

Figure 11: The Service Subscription includes an efficient four-tiered escalation process which ensures that you always have an escalation point.

The mission of Omada support is to help ensure that you get the most out of your IT investments.

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, 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.

omadaidentity.com

15092023