Omada

# Governance

## IdentityPROCESS+

**Why Governance Management is important:**

1. Ensure that users are not granted more access rights than they need to do their jobs.

2. Gives business system owners and line managers the opportunity to ensure the correct level of access

3. Enforces policies involving data protection regulations and access right conflicts

**Throughout an organization it can be extremely complex to document who has access to what and why they were granted that access. Governance ensures that identities are not granted more access than they need to do their jobs, gives application, system owners and line managers the opportunity to ensure the correct level of access, and enforces policies involving data protection regulations and access right conflicts.**

Business processes for governance allow organizations to verify who has access to what information, remove access that is no longer needed, produce real-time and historical audit reports and ensure that Segregation of Duty (SoD) policies are properly enforced.

Administrators and security practitioners need to evaluate access rights on a regular basis, otherwise users will accumulate access to more systems than they need as they change roles. Governance processes also allow for un-owned accounts (orphaned accounts) to be reassigned or deleted. Administrators can also ask data owners and managers to assign different risk classifications to data held within their respective systems. Finally, verifying that the actual state of access and entitlements matches the desired state is key to maintaining good governance.

As part of Omada IdentityPROCESS+, there are several key components to Governance that are critical to follow best practices to ensure business efficiency is optimized, security is tight, and compliance is met.

## Generate Report

Setting up reports that can provide a sense of what is actually happening is critical for success. Real-time dashboards allow organizations to understand their current access compliance situation so that they can maintain compliance. Reporting within Omada can also process extra data from the data repository to show information about relevant objects and provide a comprehensive data overview. This view allows organizations to see who has, or has had, access to what, why, and when that access was granted, who approved it, and when it was revoked.

## Perform Attestation

After reports have been set up, regularly verifying that access rights, policies, role definitions, and master data in Omada are still valid is up next. Certification campaigns (also called reviews, attestations or re-certifications) are used to periodically validate the information in Omada. Omada administrators can define the purposes of the campaign, including what data is to be certified, who should certify it, and how often a

### Process Stakeholders

Within IGA processes, it is critical that multiple stakeholders are aligned and working together. For Identity Security Breach Management, the following teams must be involved in the following capacities:

**Executive Team**

- Establish vision for Audit efforts
- Review results to ensure Audit requirements are addressed

**Policy Owners**

- Ensure that policies are aligned with business needs
- Participate in reporting and certification campaign scoring and follow-up

**Auditors**

- Define audit parameters
- Conduct the audits
- Participate in testing audit functions
- Analyze and remediate exceptions

**IGA Team**

- Configure and monitor Omada

survey should run directly in the portal. The administrator can also input what should happen when responses to the survey are submitted, or when answers are not given, as well as set notifications and reminders to be sent, and determine who can monitor and manage the campaigns and surveys.

## Administer Certification Campaign

The survey administrator can initiate and assign surveys to the relevant managers or survey owners. This includes determining when the survey starts, monitoring its ongoing progress, reassigning questions if needed, generating and sending reports and closing the survey. IdentityPROCESS+ lays out how surveys are created in the design certification campaign process and scoped based on factors such as risk classification, systems and resource types for maximum effectiveness.

## Respond to Campaign Questions

When the campaign is launched by the administrator the certification task is sent to the manager for review, so as to enable responses. Once they receive the task to recertify data (i.e. access rights for managed identities), the reviewer reviews the data and submits answers to the questions. If unable to answer some of the questions, the survey can be reassigned to another user (if the survey admin has permitted this action when launching the survey).

## Transfer Ownership

When someone leaves the company, or changes roles, the organization must transfer ownership of certain objects to another human identity. This automatically starts a workflow, which allows resource owners to propose new owners, who can accept or reject the proposal.

## Access Review for Manager / Resource Owners

As part of the ongoing process to review access, administrators and practitioners should regularly review access rights assigned to all identities. Access reviews are initiated either on a scheduled basis or done ad hoc manually by system owners or administrators. They can then verify accounts by system, organizational unit, specific resources, compliance status, or classification tags. Direct assignments are expired and deprovisioned immediately, and if a kept assignment already has a desired state it will remain as-is.

## Perform Reconciliation

Omada can check if the desired security and compliance state matches the actual access granted to system resources. If there is a mismatch, the differences need to be promptly rectified to maintain both security and compliance. Omada compares the defined desired state with actual state gathered from target systems and graphically displays compliance status; whether it is 'under control' or not, whether it has been

explicitly, or implicitly approved. Other potential states include not approved, orphan assignment, pending deprovisioning, in violation, or implicitly assigned.

## Systems and Data Store Classification

Applying classification tags to identities, systems, resources, resource folders, contexts and other objects means they can be identified when specific company processes need to be applied. This also helps to manage resources differently depending on the types of data being stored, the sensitivity of the information, and any regulations governing their use. Data administrators can create classification tag categories in Omada. For example, the classification category 'GDPR' could be populated with tags 'personal data' 'personal sensitive data' 'high-risk data' 'low-risk data' etc., thereby allowing administrators to manage different types of data according to internal policies and external requirements.

## Apply Classification Tags to Data Objects

Administrators can identify data that is held in different resources so it can be managed with the appropriate levels of security/compliance policies defined by the organization. When classification tags and tag categories are set up, data objects are tagged using a classification survey. These tags and tag categories are used to establish and operationalize the risk management strategy and put relevant controls in place. This also allows the administrator or system owner to create a survey which is sent to users, presenting them with tasks to classify the survey. Once the questions are completed, the classifications need to be approved by the category owner. Once approved, classification tags are added or removed to/from the object.

## Segregation of Duties

A critical component of Governance is the evaluation of segregation of duty policies to ensure that individuals are not granted toxic combinations of access rights that enable them to commit fraud. Administrators can create new constraint policies to determine whether toxic combinations of access rights have been assigned, can detect violations, and allow managers to evaluate the situation. Omada evaluates user identities for violations, and if found, the automated workflow sends the task to the manager for approval. If approved and a compensating control is selected, access is provisioned. This is also automatically logged and stored.

### Process Stakeholders

Within IGA processes, it is critical that multiple stakeholders are aligned and working together. For Governance, the following teams must be involved in the following capacities:

**IGA Team**

- Generate reports for compliance and security teams
- Set up attestation surveys across business systems

**Line Managers**

- View reports
- Respond to access review requests

**Business and Application System Owners**

- Use reports to determine who has access to their systems
- Generate certification campaigns to verify user access and respond to access reviews for resource owners
- Help initiate account ownership process to review orphaned account assignments and transfer them to new owners