Omada

Business Alignment

IdentityPROCESS+

Roles, Constraints, Contexts Best Practices

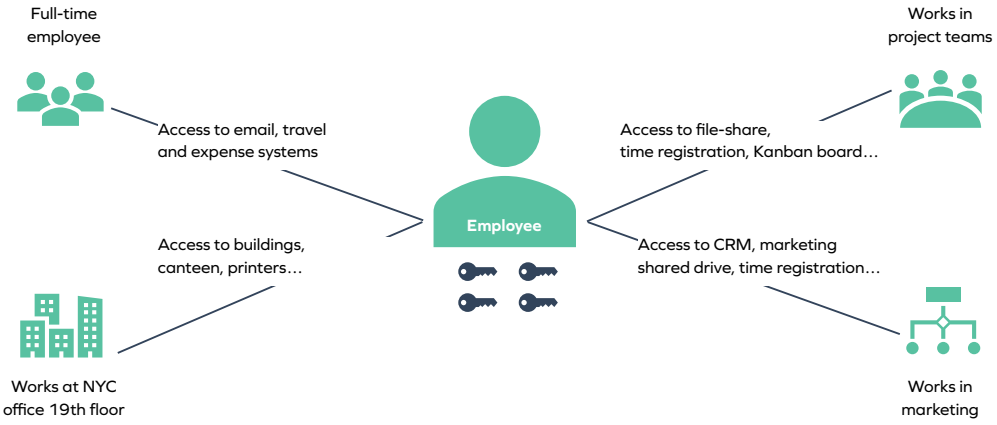
If using a role-based approach to grant access, but the role model is not sufficiently developed, the rollout of IGA will be delayed. To speed up the process of granting access rights:

- Role governance processes need to be established
- Constraints between roles should be defined at role or business process level to allow for oversight
- Access rights must be automatically revoked when a user is no longer assigned to the context, i.e. if they are working on a short-term project

Many organizations are made up of a huge number of varying identity types: employees, technical identities, contractors, devices, and end-users. If all these identities were each managed one-by-one, it would not only take a huge amount of time, effort, and resources to get under control, but also would likely result in errors along the way.

A best practice is to group identities based on their job function (roles), where they work (context), or other traits that link identities that require similar access. However, it can still be challenging to align the business under common terminology, philosophies, and technology to make this happen.

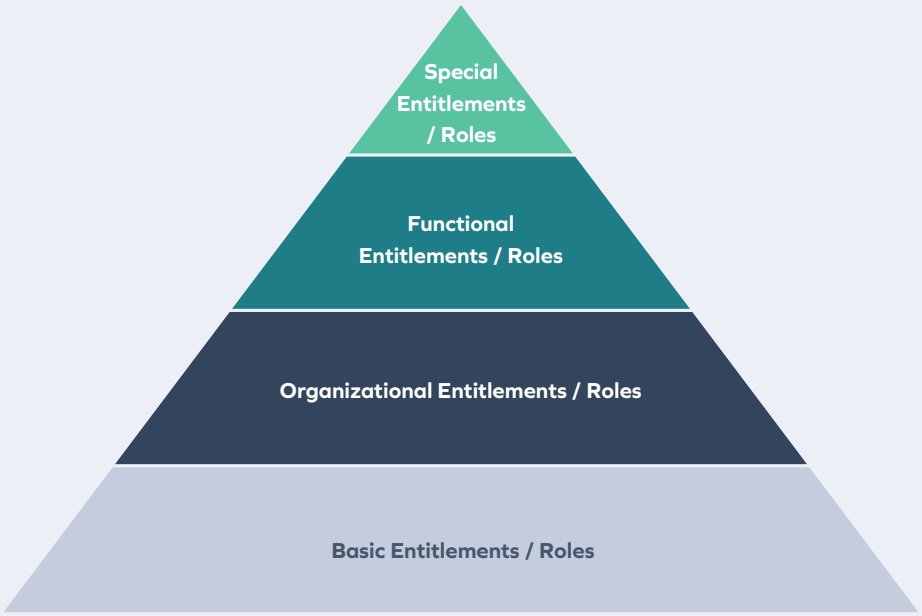
As part of Omada IdentityPROCESS+, there are several key components to Business Alignment that are critical to follow best practices so as to ensure that business efficiency is optimized, security is tight, and compliance is met.



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

Business Alignment

Within Omada IdentityPROCESS+, the Business Alignment process helps reduce the complexity of onboarding and managing employee access rights using policies, roles and contexts with predefined access rights. It starts with definition of roles, then managing policies, then contexts to build groups of users with similar access requirements that can be treated as a single entity.



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

Manage Role

First, an administrator can create a set of access rights for a common job function (a role) to increase organizational efficiency and reduce the likelihood of mistakes made when managing each identity individually. Processes outlined in IdentityPROCESS+ include the ability to create, modify, or terminate roles to allow administrators to manage descriptions of access requirements for roles. After the role has been defined, access is automatically provisioned once an identity is assigned that role. This can be modified over time to match new business requirements such as new applications being introduced. Roles created in Omada and assigned out to new employees can also be based on the job description in the HR system and information is typically shared from the HR system to Omada.

Manage Policy

After roles have been created to fit the organizational flow, creating and managing policies to provide granular access is required. Within IdentityPROCESS+, a framework is outlined to help automate access assignments based on policies. Administrators can also easily create, modify, or terminate policies as needed, and as the business changes. Assignment policies can depend on matching identity characteristics, like a US manager being granted access to the US-based expense management system versus having access to the European equivalent. In IdentityPROCESS+, the administrator can set up identity filters and create new assignment policies using the 'create new assignment policy' process. Any identities that match this filter are then automatically given access rights defined in the policy. Later, if the policy is removed, or if the identity no longer matches the filter, any access rights that were set up by it are also removed automatically. This ensures that there are no stagnant or unmonitored access rights that could create problems down the line. Policies can also be set with a 'valid from' and 'valid to' date which allows administrators to grant special access on a temporary basis. Access is automatically removed once the time expires.

Process Stakeholders

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

HR

• Ensure consistency of job titles in the HR (or other) system

Line Managers

• Help determine different roles within teams, as well as policies and contexts, across the wider organization

• Work with HR to ensure consistent job titles within their departments

System Owners

• Work with their peers and Line Managers to define toxic access combinations so constraint policies can be defined

• Classify resources and define approval requirements for access requests per resources/ systems they own

IGA Team

• Create roles, policies, and contexts once they are defined by the Line Managers

Constraint Policies

A critical component in maintaining order for identities is establishing safeguards to prevent business users from granting access to systems that enable them to commit fraud. The Business Alignment process enables administrators and security practitioners to create, modify, and delete constraint policies, like Segregation of Duty (SoD). After constraint policies are in place, they are checked each time a user submits a self-service access request or if an automated assignment is made. If a violation occurs, it is routed to a manager, or constraint owner, to determine a resolution. All activities are logged with a complete audit trail of who has been granted what type of access, and why. If a constraint policy needs to be broken, there are processes set up to ensure that it is for a legitimate reason, with strict and automated audit processes to ensure that violations and risks are mitigated by appropriate controls and regularly reviewed.

Manage Context

When users have equal access requirements due to being in the same business situation, contexts allow administrators to manage them as a single entity when assigning access rights rather than inefficiently working on them individually. Within IdentityPROCESS+, administrators can create, modify, terminate, request and approve, prolong and remove contexts. This helps to manage the grouping together of users that require the same access levels. Logical groupings can be based on any business situation such as location or project. Contexts allow greater flexibility as users are added - as opposed to roles which are predominantly based on job title. Within this process, teams can create new contexts so that users can then request membership and be granted and provisioned access automatically, with a full audit trail automatically maintained of all requests.

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