ITIL® ACCESS MANAGEMENT

ITIL 4 Guide ›

What is access management?

Access management works closely with information security management to ensure that the access provisions of the information security policy are enforced. Requests for access may be initiated as service requests and be handled by the service desk, or may be routed to a security group for fulfillment.

A major part of information security management is controlling access to applications or data. Access management is responsible for dealing with requests from users for access. This process involves username and password control, but also includes the creation of groups or roles with defined access privileges, and then controlling access by defining group membership.

In addition to granting rights, access management revokes rights when a user's status changes through transfer, resignation, or termination. Also, access management should periodically review the roles or groups used to control access to ensure that only necessary rights are being granted and that there are no rights conflicts among the roles or groups.

Download Now: ITIL 4 Best Practice e-Books

These all-new for 2020 ITIL e-books highlight important elements of ITIL 4 best practices. Quickly understand key changes and actionable concepts, written by ITIL 4 contributors.

Free Download ›

Free Download ›

Access management is also known as **identity management** or **rights management**. Its role is to make sure that the individuals in an organization are able to use the systems that help them do their job, but only have as much access to them as they really need. This process runs on the information security principle of "least privilege" (or "least authority"), which states that each user must only be able to access the information or resources necessary to their job. While it may seem like a burden to have to deny access to those users who want it, it's important for everyone to follow the process. Access management enables the organization to maintain a secure environment that not only prevents unauthorized usage, but also averts data breaches that can erode customer trust and incur financial penalties.

Access management definitions

- **Access** is the level or extent of an application's functionality that a user is allowed to use. For example, in a file server or content management system, access is whether a user can read a file, read and write a file, edit a file, or delete a file.
- **An access request** is the way in which a user requests to be able to access a service. This is usually a request for a login via a service request from the service desk.
- **The information security policy** is the document that provides the rules that access management then implements. The information security management process builds and maintains this policy. **Identity** is the information needed to tell you who a user is. It is used to verify a user's status within an organization and define his or her access levels. An identity is unique to the user.
- **Rights**, also known as privileges, are the settings that you provide to a user along with their access. For example, a user may have access to view an internal wiki but may not be allowed to edit or delete anything in the wiki.
- **Service groups** are similar sets of services. These services might perform similar or interrelated functions, such as a ticketing system and a call center system. This is implemented when users are added to a specific group that then grants similar access across multiple systems.

Access management activities

ITIL is very clear about the hierarchy of access decision-making, stating that access should be granted according to the rules set by the information security policy. Access management should not dictate any of the security policies. The activities of access management, therefore, respond according to the rules that have already been set.

Request Access

This is the first step in implementing access management. Requests can come from the service desk via a service request (in service operation) or from a request for change (in service transition). Access can involve going from not having access to having access, or from having one level of access to another level. Ideally, the service catalog should include processes for responding to requests. This activity should define who can request access, what information is required, and how the request will go through the system.

Verification

This activity verifies that an individual who requests access is qualified to ask for it. The user must prove their identity and that they have a legitimate business reason for the request. Different levels of access may include different amounts of verification. For example, access to view and edit financial reports should require much different approval requirements than the verification required to create a new user with default permissions.

Providing Rights

Once the individual has been verified, it's time to provide access. This involves adding the user to a new group, if needed. Credentials may need to be created in each system that a user requests to

access. It is the job of access management to ensure that the access provided does not interfere with any other access rights already granted. Building the catalog of user roles and access profiles helps keep the different groups straight.

Monitoring Identity Status

Identity status changes are vitally important, especially for large organizations. This is where having a repository of access that has already been given is vital. If there are too many people processing access change requests, there is a chance that access could be granted that could conflict with other access granted. Automatically monitoring security changes also ensures that access is only being granted according to policy.

Logging and Tracking Access

By logging and tracking access changes, your organization ensures that the access being granted is only used as intended. Tracking changes also protects the organization from security gaps and risks. Events such as unauthorized access, unusual application activity, and excessive incorrect login attempts should be evaluated for security breaches.

Removing or Restricting Rights

This activity involves removing access once it has been granted or restricting access based on user roles. This occurs when users change roles over the course of their employment, working in different departments or on different systems. Whether a user is terminated, dies, changes roles, moves departments, or changes physical locations, there should be a process in place for granting them the access their role should allow.These activities are the foundation of a solid information security policy. Processes should exist for each activity as it applies to each user role.

Access management processes

Access management has two sub-processes:

1. **Maintaining a catalog of user roles and access profiles:** This process involves building and maintaining an active repository of all of the user roles and access profiles within the organization. User roles are defined listings and hierarchies of all the roles in an organization, including types of users, such as service desk agent, business user, sales person, etc. It is important to review these roles periodically, particularly when requests come in for access changes that don't seem to correspond to the role. The access given to roles should also be evaluated when new software is purchased or decommissioned. This allows you to grant and remove access based on the process rather than by one-off requests.
2. **Provisioning user access requests:** This sub-process is where access management activities come into play. Access management verifies the user, provides access rights, monitors the identity status, removes or restricts access, and logs and tracks access. The success of this sub-process depends maintaining an accurate user profile and access repository.

Access management and other ITIL processes

Access management interfaces with many other stages, such as:

- Component management inside capacity management when there is a license limit that would inhibit the creation of new logins
- Financial management when adding an additional user would impose a financial cost
- Service design and service strategy when services and components are discussed and the number of logins needed must be agreed upon
- Other service operation processes when the service desk sends a request to access management

Access management is the sole process responsible for implementing security policies. As the guardian of the organization's systems, it is as vital to the health of the organization as the locks on the front door. Unfortunately, it is often one of the last formal processes to be fully fleshed out in the service operation stage of the ITIL lifecycle.