

ITIL – A guide to access management

Access management process information

Why have access management?

Access management is the process of granting authorised users the right to use a service, while preventing access to non-authorised users. Access management can also be referred to as rights management or identity management.

The objectives of access management

Access management provides the right for users to be able to use a service or group of services. Access management is, therefore, the execution of policies and actions defined in information security and availability management.

- Access management is the process of granting authorised users the right to use a service, while restricting access to non-authorised users
 - Grant access to services, service groups, data or functions
 - Only if they are entitled to that access
- Protecting Confidentiality, Integrity and Availability (CIA). Sometimes known as rights management or identity management
 - Remove access when people change roles or jobs
 - Regularly audit access permissions to ensure they are correct
- Security incidents and problems related to access management will be discreetly recorded

The scope of access management

Access management is effectively the execution of both availability and information security management, in that it enables the organisation to manage the confidentiality, availability and integrity of the organisation's data and intellectual property.

Access management ensures that users are given the right to use a service, but it does not ensure that this access is available at all agreed times – this is provided by availability management.

Access management can be initiated by a service request through the service desk.

The value to the organisation of access management

Access management provides the following value:

- Controlled access to services ensures that the organization is able to maintain more effectively the confidentiality of its information
- Employees have the right level of access to execute their jobs effectively
- There is less likelihood of errors being made in data entry or in the use of a critical service by an unskilled user (e.g. production control systems)
- The ability to audit use of services and to trace the abuse of services
- The ability more easily to revoke access rights when needed – an important security consideration
- May be needed for regulatory compliance

The activities of access management

Requesting access – Access can be requested using one or any number of mechanisms, e.g.

- A standard request
- A request for change
- A service request (submitted via the request fulfilment system)
- Executing a pre-authorised script or option
- Rules for requesting access are normally documented as part of the service catalogue

Verification – Access management needs to verify every request for access to an IT service from two perspectives:

- That the user requesting access is who they say they are
- That they have a legitimate requirement for that service

Providing rights – Access management does not decide who has access to which IT services. Access management executes the policies and regulations defined during service strategy and service design. Access management enforces decisions to restrict to provide access, rather than making the decision. As soon as a user is verified, access management will provide that user with rights to use the requested service. In most cases, this will result in a request to every team or department involved in supporting that service to take the necessary action. Ideally, these tasks should be automated.

Monitoring identity status – As users work in the organisation, their roles change as do their needs to access services, e.g. job changes, promotions/demotions, resignation or death etc. Access management should understand and document the typical user lifecycle for each type of user and use it to automate the process. Access management tools should provide features that enable a user to be moved from one state to another or from one group to another, easily and with an audit trail.

Job changes – In this case the user will possibly need access to different or additional services.

Promotions or demotions – The user will probably use the same set of services, but will need access to different levels of functionality or data.

Transfers – In this situation, the user may need access to exactly the same set of services, but in a different region with different working practices and different sets of data.

Resignation – Access needs to be completely removed.

Death – Access needs to be completely removed.

Retirement – In many organisations, an employee who retires may still have access to a limited set of services, including benefits systems or systems that allow them to purchase company products at a reduced rate, alumni information etc.

Disciplinary action – In some cases, the organisation will require a temporary restriction to prevent the user from accessing some or all of the services that they would normally have access to. There should be a feature in the process and tools to do this, rather than having to delete and reinstate the user's access rights.

Dismissals – Where an employee or contractor is dismissed, or where legal action is taken against a customer (for example, for defaulting on payment for products purchased on the internet), access should be revoked immediately. In addition, access management, working together with information security management, should take active measures to prevent and detect malicious action against the organisation from that user.

Logging and tracking access – Access management should not only respond to requests. It is also responsible for ensuring that the rights that they have provided are being properly used. Information security management plays a vital role in detecting unauthorized access and comparing it with the rights that were provided by access management. Access management may also be required to provide a record of access for specific services during forensic investigations. If a user is suspected of breaches of policy, inappropriate use of resources, or fraudulent use of data, access management may be required to provide evidence of dates, times and even content of that user's access to specific services.

Removing or restricting rights – Just as access management provides rights to use a service, it is also responsible for revoking those rights. Again, this is not a decision that it makes on its own. Access management will execute the decisions and policies made during service strategy and design and also decisions made by managers within the organisation. Removing access is usually done in the following circumstances:

- Death
- Resignation
- Dismissal
- User has changed roles etc.

Access management relationship with other ITIL processes and business processes

Access management should be linked to the human resource processes, to verify the user's identity, as well as to ensure that they are entitled to the services being requested.

Information security management is a key driver for access management as it will provide the security and data protection policies and tools needed to execute access management.

Change management plays an important role as the means to control the actual requests for access. This is because any request for access to a service is a change, although it is usually processed as a standard change or service request (possibly using a model) once the criteria for access has been agreed through service level management.

Service level management maintains the agreements for access to each service. This will include the criteria for who is entitled to access each service, what the cost of that access will be, if appropriate, and what level of access will be granted to different types of user (e.g. managers or staff).

There is also a strong relationship between access management and configuration management. The Configuration Management System can be used for data storage and interrogated to determine current access details.

The terminology of access management

Access – refers to the level and the extent of a service's functionality or data that a user is entitled to use.

Identity – refers to the information about the user that distinguishes them as an individual and which verifies their status within the organization. By definition, the identity of a user is unique to that user.

Rights – (also called privileges) refer to the actual settings whereby a user is provided access to a service or group of services. Typical rights, or level of access, include read, write, execute, change and delete.

Service or service groups – Most users do not use only one service, and users performing a similar set of activities will use a similar set of services. Instead of providing access to each service for each user separately, it is more efficient to be able to grant each user, access to the whole set of services that they are entitled to use at the same time.

Directory services – refers to a specific type of tool that is used to manage access and rights.