Access Management

Process Guide

06/03/2022

Table of Contents

Overview

All information is...

Description

Access Management is the process that is responsible for granting access rights to authorized users and removing those rights when they are no longer pertinent as per policy. This is done via the Request Fulfillment model, after the user, request and rights have been verified.

This process ensures that access is granted to and retained by only those users authorized and therefore helps to protect the confidentiality and integrity of data.

Information Security Management and Availability Management set the policies and provide guidance. Access Management is the execution of these policies.

The Service Desk provides the central point of contact for the managing, tracking and execution of the requests.

Scope

Roles

Roles are allocated to work on specific tasks within the process. The responsibilities of a role are confined to the specific process and do not imply any functional standing within the hierarchy of an organization.

The roles for this process are:

Name	Description
Requestor	The source of the request. This could be a person or a system.
Service Desk Agent	An agent on the Service Desk
Access Management Analyst	The role assigned to evaluate, verify or provide the rights for granting access.
Application Management Analyst	This role is an application specialist that may be consulted on a requested or may provide the rights request for a specific service
Operations Management Analyst	This role is an Operations specialist that may be consulted on a requested or may provide the rights request for a specific service

Name	Description
Access Management Process Manager	The Process Manager is responsible for the operational management of the process. The Process Manager's responsibilities include planning and coordination of all activities required to carry out, monitor and report on the process. Specific responsibilities include: • Managing the day to day activities of the process • Gathering and reporting on process metrics • Tracking compliance to the process • Escalating any issues with the process • Acting as chairperson for process meetings • Identifying deficiencies and developing action plans to address them • Interfacing with managers of other Service Management processes • Acting as the single point of contact for the process • Assigning work to the Analysts There may be several Process Managers for the Access Management process. The Process Manager(s) take direction from the Process Owner in order to ensure consistent execution of the process across all areas of the organization.
Access Management Process Owner	The Process Owner is accountable for the overall quality of the process, ensuring that the process is performed as documented and is meeting its objectives. The Role's responsibilities include sponsorship, design, review and continual improvement of the Process and its Metrics. Specific responsibilities include: • Defining the overall mission of the process • Establishing and communicating the mission, goals and objectives • Resolving any cross-functional (departmental) issues • Ensuring consistent execution of the process across departments • Reporting on the effectiveness of the process to senior management • Initiating any process improvement initiatives The Process Owner should be a Senior Manager with the ability and authority to ensure the process is rolled out and used by all departments within the IT organization.

RA(S)CI

Task	Access Management Analyst	Application Management Analyst	Operations Management Analyst	Requestor	Service Desk Agent
ACC 1.1 Create Access Request				R	R/A
ACC 1.2 Verify Access Request	R/A				

Task	Access Management Analyst	Application Management Analyst	Operations Management Analyst	Requestor	Service Desk Agent
ACC 1.3 Role Conflict Check	R/A	C	C	I	
ACC 1.4 Approve and Assign Request	R/A			I	
ACC 1.5 Provide/Revoke Rights	R/A	C	C		
ACC 1.6 Close Request	R/A			I	

Workflow

The Workflow section identifies the process inputs, outputs, activities and task details along with the general task flow within each activity.

Activities

An activity is a collection of tasks that are related to each other. An activity may also be constructed to support a specific objective of the process.

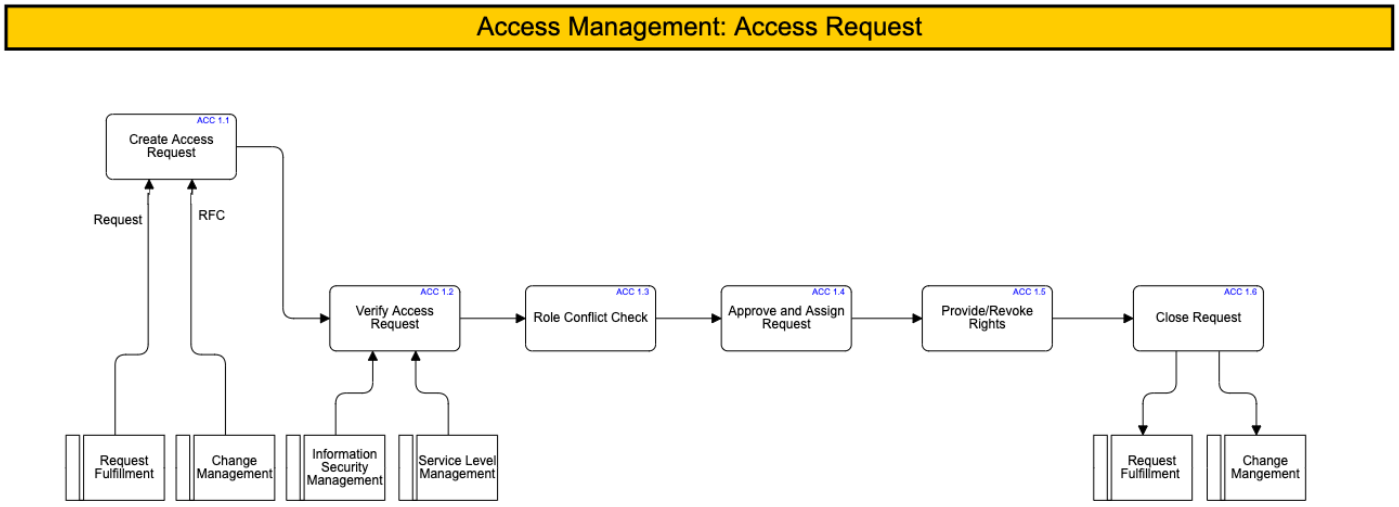
Access Request

The purpose of this activity is to manage, track and execute the request for access. The request can be to provide, revoke or modify the rights currently granted to a user. The requests submission can be manual, a manager or user can make a call to the Service Desk or submit the request via a Service Request. Automated request submissions can come from a HR System feed in response to changes in an employee's status with the organization. Request submissions may also come from Change Management in the form or tasks from an RFC.

Access Requests are managed and tracked in a Request Fulfillment model created specifically for Access Management. Requests are fulfilled using Access Management tools and procedures that have approved by Security Management policies.

All requests must be verified to ensure that both user and the requestor are valid and authorized for the rights being requested.

Cross-Functional Flow Diagram



Tasks

ACC 1.1: Create Access Request

The Access Request is nominally created by the Service Desk Agent, in response to a request made, manually or automatically, for the granting, revoking or modifying of rights to a user or users.

The request may be in the form of Service Request, a Change Request or an automated Human Resource Request from the HR service or system.

In many cases, the translation into an Access Request may be handled by automation.

Where human intervention is required, the request processing should optimally be directed to specialized Service Desk personnel unless the activity is straight forward.

The purpose of this task to collect all the required information and properly complete the request so that it can be processed effectively and efficiently.

ACC 1.2: Verify Access Request

The purpose of this task is to verify the access request. There are 2 items that must be verified. First, the user that will be recipient of the request must be verified to ensure that they are an authorized user. Second, the request must be verified to ensure that it is valid and that it came from an authorized source. The identity of the user named in the request must be verified in the HR records for internal access and the customer or supplier database if the request is for external access, unless this is available from the CMDB.

The verification of the authenticity of the request must come from a source other then the requestor. This independent verification must ensure the requestor has the authority to make this request.

If the request cannot be verified, the request is rejected and the requestor notified.

All or parts of this activity may be handled by automation.

ACC 1.3: Role Conflict Check

The rights requested in the request must be checked to ensure that they do not violate policy and that they do not conflict with other rights granted to the user. For example a user may be assigned to several roles or groups of roles. These roles must be checked to ensure that they do not grant the user access to rights that conflict with compliance regulations or provide too much authority for this user.

Any conflicts must be reported to the designated Application or Technology Support team for resolution. If the conflict cannot be resolved, the request is rejected and the requestor notified.

All or part of this activity may be handled by automation.

ACC 1.4: Approve and Assign Request

After the request has been verified and checked for conflicts, the request is approved and assigned to the correct Operation or Technical Management so that the proper rights can be assigned to the designated user.

If the request cannot be approved, the request is rejected and the requestor notified.

This activity may he handled by automation in some cases

ACC 1.5: Provide/Revoke Rights

The team (or automation) assigned the request will now make the required changes to the rights as detailed in the request. There is no more verification of the request, but the success or failure of the execution of the request must be captured and relayed back to the requestor and recorded in the request ticket.

ACC 1.6: Close Request

Upon completion, the request is closed and the requestor notified of the status of the request.

Appendix

Additional documents or information that are related to the process in some manner

Definitions

Definitions for unique terms related to the process that may aid in the understanding of the process and its documentation

Term	Definition
Access	The scope of capability and level of functionality within a service that a user is able to employ
Identity	The information about an individual that distinguishes them from all other individuals and which describes their role(s) and status(es) within the organization. The identity of the individual is unique to that individual. The term "user" should be considered equated with "individual" in this context. Initial identification of an individual typically requires multiple pieces of information such as Name, address, other contact information, identification document (passport, driver's license, etc.), identification number (e.g., employee number SSN), biometric data (e.g., DNA profile, thumb print, retinal pattern, voice pattern, etc.). Identities needs to be defined for various parties who require access to services and data including employees, contractors, vendor personnel, customers and representatives of various regulatory and investigative bodies. Once an individual's identification has been initially confirmed they are normally issued (or may self-issue) a unique identifier within the organization (a userid) and are issued (and/or self issue) a password. Subsequent confirmation of identity when attempting to access services will usually be a combination of factors commensurate with the security levels required for that service or the data to be accessed.
Rights	The actual parameter settings that provide a type of access for an individual for a service or data components within a service. "Privileges" should be considered a synonym of "Rights".
Groups	While each user and each service can be treated as an individual, for administrative purposes, users and services are usually grouped. There can be User groups, Roles, Service groups, etc. The most common maps between these can be set up as "profiles" with any unique requirements applied for seperately. Access Management will maintain a catalog of these profiles (usually in conjunction with HR) to simplify the requesting and removal of access.

Term	Definition
Access Management	The process of permitting authorized individuals to use components of a service and preventing non-authorized individuals from so doing. Synonyms are "Identity Management" and "Rights Management" It handles some of the operational aspects of both Information Security and Availability Management. From an Availability Management point of view, Access Management ensures authorized users to have the right of access to services but has nothing to do with ensuring that those services are available to them. From an Information Security Management point of view, Access Management ensures that Information Security access policies are applied thoroughly, consistently and in a timely manner through service, organizational, customer, supplier and user changes, but plays only a supporting role in the detection of unauthorized access and the subsequent damage containment and recovery which remains within the responsibility of Information Security Management.
RACI Model	The RACI Model is based on the principle that people act in one of four ways when executing a task. It accounts for the fact that more than one role may be active in performing a specific task while clearly defining specific responsibilities for that role. While many roles may be involved in a task only one is Accountable for the results. The actions are: R Responsible for the action (may do the task) A Accountable for the action (including approval) C Required to be Consulted on the action I Required to be Informed of the action If a task does not have an Accountable role indicated then the Responsible role is assumed to be accountable for the task.