Software Engineering Institute

CERT® Resilience Management Model, Version 1.2

Access Management (AM)

Richard A. Caralli
Julia H. Allen
David W. White
Lisa R. Young
Nader Mehravari
Pamela D. Curtis

February 2016

CERT Program

http://www.cert.org/resilience/

Carnegie Mellon

This material is based upon work funded and supported by various entities under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of Various or the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM-0003234

ACCESS MANAGEMENT

Operations

Purpose

The purpose of Access Management is to ensure that access granted to organizational assets is commensurate with their business and resilience requirements.

Introductory Notes

In order to support services, assets such as information, technology, and facilities must be made available (accessible) for use. This requires that persons (employees and contractors), objects (such as systems), and entities (such as business partners) have sufficient (but not excessive) levels of access to these assets.

Effective access management requires balancing organizational needs against the appropriate level of controls based on an asset’s resilience requirements and business objectives. Insufficient access may translate into higher levels of asset protection but may impede the organization’s ability to use the assets to their productive capacity. On the other hand, excessive levels of access (due to inadequate levels of control) expose assets to potential unauthorized or inadvertent misuse, which may diminish their productive capacity. Finding the right level of access for persons, objects, and entities so that they can perform their job responsibilities while satisfying the protection needs for the asset is a process that involves business owners, organizational units, and the owners and custodians of assets. In essence, these parties must come to agreement on what level of protection is sufficient given the need to meet objectives. Access management encompasses the processes that the organization uses to address this balancing act.

Access privileges and restrictions are the mechanisms for linking persons, objects, and entities (and their organizational roles) to the assets they need to perform their responsibilities. Access privileges and restrictions are operationalized (i.e., made operational or implemented) through logical and physical *access controls*, which may be administrative, technical, or physical in nature and can be discretionary (i.e., at the will of the asset owner) or mandatory (constrained by policies, regulations, and laws).

Access controls differ significantly from access privileges and restrictions. In the purest sense, an access control is the administrative, technical, or physical mechanism that provides a gate at which identities must present proper credentials to pass. Some examples of access controls are access and security policies, access control lists in application systems and databases, and key card and key pad readers for facilities. Access controls are established relative to the resilience requirements for an asset and service they protect—they are the mechanism that enforces the resilience requirements of confidentiality, integrity, and availability. When an identity presents an access request to an access control, and the identity has the necessary credentials required by the control (i.e., is authenticated and authorized to have the level of access requested), access is provided.

Access controls are a key element of the protection provided to an asset and form a substantial portion of the organization’s protection strategy for assets and services. Because the operational environment is constantly changing, it is difficult for an organization to keep access controls current and reflective of actual business and resilience requirements. The Access Management process area establishes processes to ensure that access to organizational assets remains consistent with the business and resilience requirements of those assets even as the organization’s operating environment changes. At a summary level, this includes activities to

- involve owners of assets in the process of establishing and maintaining access privileges
- manage changes to access privileges as the identities, user roles, business requirements, and resilience requirements change
- monitor and analyze relationships between identities, roles, and current access privileges to ensure alignment with business and resilience requirements
- adjust access privileges when they are not aligned with business and resilience requirements
- ensure that the access privileges granted to a user by the system of access controls reflect the privileges assigned by the asset owner

Clearly, access management is strongly tied to identity management. In identity management, persons, objects, and entities are established as identities that may require some level of access to organizational assets. However, access privileges and restrictions are tied to identities by the roles that are attributed to the identities. Thus, as identities change, or as their roles change, there is a cascading effect on access privileges that must be managed. For example:

- New identities may be established that must be provided access privileges.
- The access privileges of existing identities may have to be changed as the job responsibilities associated with the identity change.
- The access privileges of existing identities may have to be eliminated or deprovisioned as job responsibilities expire (either through new assignments or voluntary or involuntary termination).

The selection of the appropriate access controls to enforce those rights for a given asset is outside of the scope of this process area. These activities are performed in the operations process area associated with each type of asset (e.g., Knowledge and Information Management for information assets). *(Overall management of the organization’s internal control system is addressed in the Controls Management process area.)*

Related Process Areas

The creation, maintenance, and deprovisioning of identities and their associated attributes are addressed in the Identity Management process area.

The selection and implementation of appropriate access controls for assets are addressed in the Knowledge and Information Management process area (for information), the Technology Management process area (for technology assets), and the Environmental Control process area (for facilities).

The analysis and mitigation of risks related to inappropriate or excessive levels of access privileges are addressed in the Risk Management process area.

Summary of Specific Goals and Practices

Goals	Practices
AM:SG1 Manage and Control Access	AM:SG1.SP1 Enable Access
	AM:SG1.SP2 Manage Changes to Access Privileges
	AM:SG1.SP3 Periodically Review and Maintain Access Privileges
	AM:SG1.SP4 Correct Inconsistencies

Specific Practices by Goal

AM:SG1 Manage and Control Access

Access granted to organizational assets is managed and controlled.

Access privileges describe and define a level of access to an organizational asset—information, technology, or facilities—commensurate with an identity's job responsibilities and the business and resilience requirements of the asset. In other words, access privileges define what assets identities can access and what they can do when they access these assets. Access privileges must be closely managed in order to prevent vulnerabilities that could lead to unauthorized and inadvertent misuse of organizational assets.

To manage and control access privileges, the organization must establish processes for approving and assigning these privileges, managing changes to them, and monitoring and analyzing the current access environment to ensure that it is in alignment with business and resilience requirements and does not result in additional risk to organizational assets.

AM:SG1.SP1 Enable Access

Appropriate access to organizational assets is established based on resilience requirements and appropriate approvals.

Access privileges and restrictions describe the level and extent of access provided to identities. Access privileges should be commensurate with the various roles represented by an identity but concurrently must be congruent with the resilience requirements of the assets to which the privileges are granted.

Access privileges are assigned and approved by asset owners based on the role of the person, object, or entity that is requesting access. Asset owners are the persons or organizational units, internal or external to the organization, that have primary responsibility for the viability, productivity, and resilience of a high-value organizational asset. It is the owner's responsibility to ensure that requirements for protecting and sustaining assets are defined for assets under the owner's control. In part, these requirements are satisfied by defining and assigning access privileges that are commensurate with the requirements. Therefore, the asset owner is responsible for granting and revoking access privileges to an identity based on the identity's role *and* the asset's resilience requirements. To be successful, asset owners must be aware of identities that need access to their assets and must evaluate the need with respect to business and resilience requirements before granting approval.

The organization must have processes in place to support the access request and approval process. This process begins with the registration of an identity *(as detailed in the Identity Management process area)* and then proceeds with assigning access privileges. In some cases, these activities may occur simultaneously. When assigning access privileges, the organization should have processes in place to allow

- the owners or sponsors of identities to request access (type and extent) from owners of organizational assets
- asset owners to determine the appropriate type and extent of access based on the identity's role
- asset owners to approve and grant access privileges

Access privileges are usually focused on three common types of assets: information, technology, and facilities.

- Information assets may be physical (such as paper files) or electronic (databases). The types of access privileges assigned for information assets typically include inquire, modify or change, and delete.
- Technology assets span the physical and electronic realm and cover a significantly diverse set of organizational assets.

  These are examples of technology assets:

  - all types of software, such as application systems and operating systems, including any remote software that is not contained in an organization-controlled facility but is used or accessed by the organization's users
  - all types of hardware, such as personal computers, servers, network components, telecommunications components, and peripheral devices such as routers and disk storage devices, including any remote hardware that is not contained in an organization-controlled facility but is used or accessed by the organization's users
  - networks and other shared communication devices, including fax machines

  Access to technology assets can be physical but also logical (by allowing a person, object, or entity to log on to a server or network). Logical and physical access may allow a person to modify or change a hardware or software configuration or permit removal or destruction of a technology asset.
- Facilities are buildings and other physical plant. Access privileges for physical assets generally provide or prevent entry to the facility and may limit the time period for which entry is permitted. Access privileges for facilities may be combined with access privileges for information and technology assets. This would be operationalized by allowing entry to the places where these assets are located or stored.

It should also be noted that not all access privileges are equal. In some cases, privileges are special or universal, providing trusted levels of access that are not generally provided unless the person, object, or entity is in a trusted or privileged position. Examples of such privileges include the ability to change the access control list on a file folder in a file sharing system and the possession of system administration privileges. As with general access rights, identities that request special privileges must have the approval of the owner of the assets that could be affected by the special rights.

The granting of access privileges should not be confused with the implementation of access controls. For example, an identity may be provided an appropriate and approved level of access to an organizational asset (such as permission to alter medical records), but the controls implemented over the asset may be insufficient to accommodate the privilege (such as access controls for "read" access only).

Typical work products

1. Access requests
2. Access approval
3. Access control policy
4. Access rights and responsibilities
5. Access acknowledgment

Subpractices

1. Establish access management policies and procedures.

   The organization should establish policies and procedures for requesting, approving, and providing access for persons, objects, and entities. The access management policy should establish the responsibilities of requestors, asset owners, and asset custodians (who typically are called upon to implement access requests). The policy should cover all affected assets—information, technology, and facilities—and address clear guidelines for access requests that originate externally to the organization (i.e., from contractors or business partners). The policy should also cover the type and extent of access that will be provided to objects such as systems and processes.

   The types of documentation required to fulfill the access management policy should be described and exhibited in the policy.

   The access management policy should be communicated to all who need to know, and their responsibilities should be clearly detailed in the policy. The policy should also describe disciplinary measures for violations of the policy.

2. Complete and submit access requests.

   Access requests should be sponsored by an appropriate person in the organization (i.e., a supervisor or manager) and should be directly submitted to and approved by the owner of the assets (or the agents of the owner) to which access is being requested.

   Access requests should include proper justification for the request and should be approved by the sponsor of the request.

3. Approve access requests.

   Access should be granted in accordance with the justification for the request and the resilience requirements that have been established for the asset. Asset owners are responsible for reviewing the request, justification, and resilience requirements to decide whether to approve or deny access. The access provided should be commensurate with and not exceed the requestor's job responsibilities. If possible, the approval for the access should be limited to a specific time period (one week, one month, one year), to prevent the privilege from extending beyond the requestor's need.

Limiting the term of the approval also provides the asset owner a chance to review privileges when they come up for renewal and to make changes if necessary.

If the custodian of the asset is different from the owner, the owner should communicate in writing the approval for the request as well as any modifications of the request that the owner deems appropriate given the review of the request. Access requests should not be forwarded to custodians for implementation unless they have been approved by asset owners.

If an asset owner decides to extend access rights that exceed stated resilience requirements or extend beyond the need established by the requestor's job responsibilities, the owner should document this decision and identify any potential risk that may occur as a result. Risks should be addressed through the organization's formal risk management process.

4. Provide users (access holders) with a written statement of their access rights and responsibilities.

Users should be required to acknowledge (in writing) that they understand their access privileges and will not exploit these privileges or any privileges that they have not been assigned.

5. Implement access requests.

Access requests should be provided to custodians or others in the organization who are authorized to implement access privileges.

Custodians should be part of the approval process and should sign the access request when the privilege has been implemented.

AM:SG1.SP2 Manage Changes to Access Privileges

Changes to access privileges are managed as assets, roles, and resilience requirements change.

The continual evolution of the operational environment and the identity community (persons, objects, and entities) requires constant changes to be made to access privileges to organizational assets. There are many different scenarios that may result in legitimate changes to access privileges, such as

- changes in job responsibilities and roles, such as when employees are promoted, take other positions in the organization, or leave the organization
- changes to outsourcing arrangements or the roles of external contractors
- changes to internal and external systems and processes that access organizational assets
- changes in the identity community (i.e., addition or deletion of identity, changes to the identity's roles) *(Changes to the identity community are addressed in ID:SG2.SP1 in the Identity Management process area.)*
- changes to the assets to which access privileges are provided and/or changes to the resilience requirements of the assets (which could cascade through all access privileges)

- periodic review and maintenance of access privileges (as described in AM:SG2.SP3)

In order to get a handle on this ever-changing environment, the organization must establish criteria to determine when a change in the operational environment would trigger a change in access privileges.

Owners of organizational assets have a role in the change management of access privileges. Owners are responsible for initiating and approving changes as required *before* corresponding access controls are modified to accommodate the changes. This may involve communication between asset owners and asset custodians who are responsible for implementing and maintaining those access controls. Owners are also responsible for following up to ensure that access privileges have been granted only to the approved limit.

There may also be planned changes to access privileges that must be considered. Planned changes may occur when normal operations are suspended due to a disaster or crisis. When this occurs, users may need additional privileges to perform roles that are not in their usual job responsibilities. These planned changes should be considered and approved in advance so that they can be implemented quickly when necessary. The organization should also have processes for returning user access to normal operations when the need for special privileges has been terminated.

Note: This practice is typically tied to or affected directly by changes in identities or identity profiles. Thus, the organization should consider performing this practice in conjunction with ID:SG2.SP1 in the Identity Management process area.

Typical work products

1. Documented change management processes for access control systems
2. Access privileges change criteria
3. Authorization for change in access privileges

Subpractices

1. Establish an enterprise-wide change management process for access privileges.

   In many organizations, the human resources and legal departments can be effective clearinghouses for changes to access privileges. Human resources departments are often the first to be notified of a change in an employee’s job responsibilities or the addition of new employees. These actions often translate into direct changes in access privileges. Legal departments, on the other hand, often have access to contract information that provides external entities and agencies with access privileges and may be informed of changes in these relationships that would warrant access privilege changes.

2. Establish organizational criteria that may signify changes in access privileges.

Change criteria can help the organization to determine the types of changes that must be monitored in an attempt to identify inconsistencies between identities and the privileges that have been assigned to them.

Examples of change criteria that can be useful for this purpose can be found in ID:SG2.SP1 subpractice 1 in the Identity Management process area.

3. Manage changes to access privileges.

Typically, the activities related to altering access privileges fall to custodians who implement controls commensurate with resilience requirements. Asset owners must stay informed about changes in access privileges related to the assets under their ownership and care and should notify custodians to make changes commensurately. Custodians should not make changes to access privileges for any reason without authorization and approval from asset owners.

Changes that are detected through human resources and legal processes should also be referred to asset owners for review and approval before any actions are taken by custodians.

AM:SG1.SP3 Periodically Review and Maintain Access Privileges

Periodic review is performed to identify excessive or inappropriate levels of access privileges.

Constant change in the operational environment creates the potential that at any time the current level of access provided to persons, objects, and entities (as reflected in access privileges) may not match the current level of need based on business and resilience requirements. In other words, the privileges provided to identities are out of synch with what they *should be* allowed to do. This provides a fertile ground where vulnerabilities to organizational assets can breed and be exploited.

Typically, this misalignment is a by-product of staff members switching jobs or roles—they often retain the privileges they had in the former role and are provided new privileges to support their new role. When this happens, the former privileges may continue to be used (perhaps for unauthorized purposes) and could result in fraud, collusion, or other exposures. In addition, over time access privileges that are not terminated when the need for those privileges expires provide entry points from which internal and external actors can exploit organizational assets. These types of vulnerabilities are controllable by the organization if it implements proper change control processes for access privileges.

Periodic review of access rights is the primary responsibility of the owners of organizational assets. They must ensure that the requirements they have set for their assets are being implemented through proper assignment of access privileges and implementation of corresponding access controls. Owners are also responsible for taking action whenever access rights do not correspond with legitimate identity needs and existing resilience requirements. This requires that the owners have frequent conversations with asset custodians to ensure that access controls are accordingly modified if necessary.

During periodic review, there are two particular problems that owners of assets should be attuned to:

- The first is misalignment between existing access privileges and the resilience requirements established for the assets. In this case, access privileges that have been provisioned to identities violate the resilience requirements that owners have set for the assets.
- The second is misalignment between existing access privileges and the roles and job responsibilities of the identities that possess the privileges. In this case, there is no violation of the resilience requirements, but privileges that are more extensive than necessary have been provisioned to identities that do not require this level of access.

The organization must determine the appropriate time intervals for reviewing access privileges based on the potential vulnerabilities and risks that may result from misalignment.

Typical work products

1. Guidelines and timetables for access privilege review
2. List of excessive or inappropriate access privileges
3. Documentation of actions proposed and taken

Subpractices

1. Establish regular review cycle and process.

   The mismanagement of access privileges is a major source of potential risks and vulnerabilities to the organization. Because assets and the identity community that needs access to the assets are pervasive across the organization, and in some cases extend beyond the organization, the ability to ensure that only authorized identities have appropriate privileges is an ongoing challenge. The organization must establish responsibility for regular review of access privileges and a process for correcting inconsistencies.

   The review cycle should consider the potential risks of excessive privileges as input to the time interval for performing regular review. Where access privileges provide special rights (such as “superusers”), the review cycle may have to be more frequent.

2. Perform periodic review of access privileges by asset.

   Periodic review of access rights is the responsibility of the owners of organizational assets. Reviews should be performed in accordance with the time intervals determined in AM:SG1.SP3 subpractice 1. Failure to perform these reviews on a regular basis should subject asset owners to disciplinary measures.

   In addition to identifying inconsistencies and misalignment, periodic review should also be performed to reaffirm the current need for access privileges.

3. Identify inconsistencies or misalignment in access privileges.

   Asset owners should document any inconsistencies or misalignment in access privileges. Owners should identify privileges that are

   - excessive

- out of alignment with the identity’s role or job responsibility
- assigned but never approved by the asset owner
- in violation of the asset’s resilience requirements

Owners should also identify identities that may have been provisioned with access privileges but are no longer considered as valid identities.

A disposition for each inconsistency or misalignment should be documented, as well as the actions that have to be taken to correct these issues.

AM:SG1.SP4 Correct Inconsistencies

Excessive or inappropriate levels of access privileges are corrected.

Excessive or inappropriate levels of access privileges must be corrected in a timely manner to avoid exposing the organization to additional risk. The longer that these privileges are allowed, the greater the potential that they will be exploited by unauthorized or inadvertent actions.

As a result of periodic review, asset owners may authorize custodians to take one or more of these actions:

- Change, disable, or deprovision access privileges to better reflect the identity’s role and job responsibilities.
- Disable or deprovision certain privileges to preserve resilience requirements.
- Deprovision an identity that is no longer valid. *(This action is addressed in ID:SG2.SP3 in the Identity Management process area.)*
- Take no action, but identify and characterize resulting risks and develop an appropriate response strategy.

These corrections apply to the privileges extended to any identity that exists outside of the organization’s direct control, such as business partners and suppliers.

Typical work products

1. Written authorization for changes
2. Justification for not taking corrective action
3. Access privileges to be deprovisioned
4. Risk statements
5. Correction status

Subpractices

1. Develop corrective actions to address excessive or inappropriate levels of access privileges.

   Corrective actions must be initiated by asset owners and should involve asset custodians to determine the best course of action for the organization.

2. Correct access privileges as required.

   Generally, review of access privileges will result in disabling or deprovisioning privileges. (Disabling privileges typically occurs when the need for the privilege is temporarily unjustified but may be justifiable in the future.) In a few cases, the asset owner may request a change to an access privilege instead, such as reducing the current level or extent of privileges.

   Typically, the activities related to changing, disabling, or deprovisioning access privileges fall to custodians who implement controls commensurate with resilience requirements. Asset owners should notify custodians to make changes as described in their documentation of issues and corrective action. Custodians should not make changes to access privileges for any reason without written authorization and approval from asset owners.

   Changes that are detected through human resources and legal processes should also be referred to asset owners for review and approval before any actions are taken by custodians. Detection and referral should also be performed for access privileges that must be deprovisioned due to the deprovisioning of an identity.

   Identities that have been found to be no longer valid should be deprovisioned. *(Deprovisioning of identities is addressed in ID:SG2.SP3 in the Identity Management process area.)*

3. Document disposition for excessive or inappropriate levels of access privileges that will not result in changes or deprovisioning.

   In some cases, asset owners may decide to take no action. In such a case, the asset owner should document the justification for taking no action and identify resulting risks. *(See AM:SG1.SP4 subpractice 4.)*

4. Identify risks related to excessive or inappropriate levels of access privileges.

   Risks related to allowing excessive or unjustified levels of access privileges must be analyzed and addressed so that they do not affect the organization's operational resilience. Asset owners who permit access privileges that do not align with resilience requirements or that are excessive considering the identity's job responsibilities and role should document and address risks according to the organization's risk management process. At a minimum, asset owners should be required to document a risk profile and statement regarding the access privileges.

   Risks are addressed and managed in the Risk Management process area.

5. Update status on corrective actions.

   The organization should perform status checks for all actions related to excessive or inappropriate levels of access privileges to ensure that a proper disposition is provided for each.

Elaborated Generic Practices by Goal

Refer to the Generic Goals and Practices document in Appendix A for general guidance that applies to all process areas. This section provides elaborations relative to the application of the Generic Goals and Practices to the Access Management process area.

AM:GG1 Achieve Specific Goals

The operational resilience management system supports and enables achievement of the specific goals of the Access Management process area by transforming identifiable input work products to produce identifiable output work products.

AM:GG1.GP1 Perform Specific Practices

Perform the specific practices of the Access Management process area to develop work products and provide services to achieve the specific goals of the process area.

Elaboration:

Specific practices AM:SG1.SP1 through AM:SG1.SP4 are performed to achieve the goals of the access management process.

AM:GG2 Institutionalize a Managed Process

Access management is institutionalized as a managed process.

AM:GG2.GP1 Establish Process Governance

Establish and maintain governance over the planning and performance of the access management process.

Refer to the Enterprise Focus process area for more information about providing sponsorship and oversight to the access management process.

Subpractices

1. Establish governance over process activities.

Elaboration:

Governance over the access management process may be exhibited by

- developing and publicizing higher level managers' objectives and requirements for the process
- sponsoring process policies, procedures, standards, and guidelines, including those for requesting and approving access privileges
- providing guidance for resolving access inconsistencies and repeated violations of access policy
- making higher level managers aware of applicable compliance obligations related to the process and regularly reporting on the organization's satisfaction of these obligations to higher level managers
- sponsoring and funding process activities
- verifying that the process supports strategic resilience objectives and is focused on the assets and services that are of the highest relative value in meeting strategic objectives
- regular reporting from organizational units to higher level managers on process activities and results
- creating dedicated higher level management feedback loops on decisions about the process and recommendations for improving the process

- providing input on identifying, assessing, and managing operational risks to assets, including those related to inappropriate or excessive levels of access privileges
- conducting regular internal and external audits and related reporting to audit committees on process effectiveness
- creating formal programs to measure the effectiveness of process activities and reporting these measurements to higher level managers

2. Develop and publish organizational policy for the process.

   Elaboration:

   The access management policy should address

   - responsibility, authority, and ownership for performing process activities, including requesting, approving, and providing access to persons, objects, and entities
   - the responsibilities of requestors, asset owners, and asset custodians
   - all affected assets—information, technology, and facilities
   - access requests that originate from outside of the organization
   - procedures, standards, and guidelines for
     - approving and provisioning access privileges
     - approving and provisioning special access privileges that provide trusted levels of access
     - providing change management over access privileges
     - identifying and addressing inconsistencies between approved and granted privileges
     - enforcing disciplinary actions for violations of the access policy
   - requirements for periodically reconciling access privileges and identifying inappropriate access
   - methods for measuring adherence to policy, exceptions granted, and policy violations

   Refer to AM:SG1.SP1 subpractice 1 for a description of policies and procedures for access management.

AM:GG2.GP2 Plan the Process

Establish and maintain the plan for performing the access management process.

Elaboration:

For practical purposes, access management is likely to be a highly decentralized activity that is specific to the type of asset (information, technology, or facilities) being accessed. For this reason, the organization may have a plan that covers the general management of access to organizational assets but also specific plans that address the special considerations unique to each type of asset.

Of importance in AM:GG2.GP2 is that the organization understands what plans have to be developed and that these plans are created accordingly. The plan (or plans) should be directly influenced by the organization's resilience requirements and should focus on how the organization can manage access privileges and access controls relative to its unique blend of assets and the extent of access requests and identities.

Subpractices

1. Define and document the plan for performing the process.

   Elaboration:

   In the case where plans are developed specific to an asset type (information, technology, or facilities) or access type (logical or physical), these plans should be coordinated and should reflect the organization's overall plan for access management.

2. Define and document the process description.
3. Review the plan with relevant stakeholders and get their agreement.
4. Revise the plan as necessary.

AM:GG2.GP3 Provide Resources

Provide adequate resources for performing the access management process, developing the work products, and providing the services of the process.

Subpractices

1. Staff the process.

   Elaboration:

   Staffing the access management process will likely cross many organizational lines. Access management involves organizational unit staff (such as asset owners) as well as information technology staff (such as those who implement and manage access controls for information and technology assets as directed by asset owners). Access management may also involve physical security staff such as security guards and those who implement and manage physical access controls for facilities. Information technology staff may also be involved in physical access management where systems and technology are used to implement physical access controls.

   These are examples of staff required to perform the access management process:

   - staff responsible for submitting access requests, such as supervisors, managers, and identity owners
   - asset owners responsible for reviewing and approving access requests, ensuring that access privileges and controls are commensurate with job roles and responsibilities and are not inappropriate or excessive
   - asset custodians responsible for implementing access requests and controls as directed by asset owners
   - users who have been granted access privileges
   - staff responsible for managing changes to access privileges, including human resources and legal departments
   - asset owners responsible for conducting regular reviews of access privileges by asset, identifying inconsistencies, and correcting or justifying them
   - staff responsible for developing process plans and programs and ensuring they are aligned with stakeholder requirements and needs

- staff responsible for managing external entities that have contractual obligations for process activities
- owners and custodians of high-value assets that support the accomplishment of operational resilience management objectives
- internal and external auditors responsible for reporting to appropriate committees on process effectiveness

Refer to the Organizational Training and Awareness process area for information about training staff for resilience roles and responsibilities.

Refer to the Human Resource Management process area for information about acquiring staff to fulfill roles and responsibilities.

2. Fund the process.

   Refer to the Financial Resource Management process area for information about budgeting for, funding, and accounting for access management.

3. Provide necessary tools, techniques, and methods to perform the process.

   Elaboration:

   Tools, techniques, and methods will likely involve those that help the organization implement and manage the creation and approval of access requests and the change management of access privileges.

   For AM:GG2.GP3 subpractice 3, tools, techniques, and methods do not include those necessary to implement and manage administrative (policy), technical, and physical access controls.

   These are examples of tools, techniques, and methods to support the access management process:

   - access request and approval management systems and methods
   - tools and techniques that aid in associating roles, responsibilities, identities, and access privileges, by asset owner and by asset type
   - access privilege database systems
   - tools and techniques that assist in reviewing access privileges by asset, by asset type, by asset owner, and by user
   - access privilege change management tools and methods
   - tools and techniques that assist in managing the list of excessive or inappropriate access privileges and tracking resolution actions to closure

Refer to the Knowledge and Information Management, Technology Management, and Environmental Control process areas for practices related to implementing and managing controls for information, technology, and facilities assets, respectively.

AM:GG2.GP4 Assign Responsibility

Assign responsibility and authority for performing the access management process, developing the work products, and providing the services of the process.

Refer to the Human Resource Management process area for more information about establishing resilience as a job responsibility, developing resilience performance goals and objectives, and measuring and assessing performance against these goals and objectives.

Subpractices

1. Assign responsibility and authority for performing the process.

   Elaboration:

   Responsibility for performing and managing the access management process may be distributed across the organization and may involve both organizational units and information technology. Responsibility may be delineated between access approval and authorization processes and the implementation and management of access controls. Organizational unit managers (and specifically asset owners) are typically responsible for the approval and authorization processes, while information technology and physical security staff are responsible for the implementation and management of access controls. Change management for access privileges is typically a shared responsibility among organizational units, information technology, and physical security because they must coordinate activities to ensure that privileges are approved for only authorized staff.

   AM:GG2.GP4 subpractice 1 does not specifically cover responsibility for the development and implementation of access controls for information, technology, or facilities. AM:GG2.GP4 subpractice 1 is limited to responsibility for the approval of access privileges and the management of changes to access privileges.

   Refer to the Knowledge and Information Management, Technology Management, and Environmental Control process areas for information about developing and implementing access controls for information, technology, and facilities assets, respectively.

2. Assign responsibility and authority for performing the specific tasks of the process.

   Elaboration:

   Responsibility and authority for performing access management tasks can be formalized by

   - defining roles and responsibilities in the process plan
   - including process tasks and responsibility for those tasks in specific job descriptions
   - developing policy requiring organizational unit managers, line of business managers, project managers, and asset and service owners and custodians to participate in and derive benefit from the process for assets and services under their ownership or custodianship
   - developing policy requiring asset custodians (including information technology staff) to perform process activities relative to organizational unit and asset owner instructions
   - acknowledgment of access policy by users and other identities that request access (to affirm their responsibilities in the process)
   - including process tasks in staff performance management goals and objectives with requisite measurement of progress against those goals

- developing and implementing contractual instruments (including service level agreements) with external entities to establish responsibility and authority for performing process tasks on outsourced functions
- including process tasks in measuring performance of external entities against contractual instruments

Refer to the External Dependencies Management process area for additional details about managing relationships with external entities.

3. Confirm that people assigned with responsibility and authority understand it and are willing and able to accept it.

AM:GG2.GP5 Train People

Train the people performing or supporting the access management process as needed.

Refer to the Organizational Training and Awareness process area for more information about training the people performing or supporting the process.

Refer to the Human Resource Management process area for more information about inventorying skill sets, establishing a skill set baseline, identifying required skill sets, and measuring and addressing skill deficiencies.

Subpractices

1. Identify process skill needs.

Elaboration:

Skill needs relative to AM:GG2.GP5 subpractice 1 do not include the implementation and management of access controls, which may require extensive skill levels. These skill needs are addressed in the process areas relative to each of the asset types as specified in AM:GG2.GP4 subpractice 1.

These are examples of skills required in the access management process:

- knowledge of the tools, techniques, and methods necessary to manage access privileges, including those necessary to perform the process using the selected methods, techniques, and tools identified in AM:GG2.GP3 subpractice 3
- knowledge unique to each type of asset that is required to establish and maintain privileges for each type
- knowledge necessary to work effectively with asset owners and custodians
- knowledge necessary to elicit and prioritize stakeholder requirements and needs and interpret them to develop effective requirements, plans, and programs for the process

2. Identify process skill gaps based on available resources and their current skill levels.

3. Identify training opportunities to address skill gaps.

Elaboration:

These are examples of training topics:

- understanding service desk procedures for handling access requests
- documenting, processing, routing, reviewing, and approving access requests

- ensuring access privileges are properly associated with roles, rights, responsibilities, and identities
- managing and controlling changes to access privileges and supporting databases
- deprovisioning access privileges
- supporting asset owners and custodians in understanding the process and their roles and responsibilities with respect to its activities

4. Provide training and review the training needs as necessary.

AM:GG2.GP6 Control Work Products

Place designated work products of the access management process under appropriate levels of control.

Elaboration:

AM:SG1.SP2 addresses the change control process over access privileges. However, other work products of the access management process (such as access requests and access policy acknowledgments) must also be managed and controlled.

Tools, techniques, and methods should be employed to support the initiation, approval, and acceptance of access requests and corresponding access privileges. Access privileges are operationalized using access control mechanisms. For example, an access privilege allowing modification of information may be represented by an entry in a file's access control list. Thus, managing work products such as access privileges may necessarily involve management of the access controls themselves, even though access controls are not within the scope of AM:GG2.GP6.

These are examples of access management work products placed under control:

- access control policy and acknowledgments from users that they understand and will abide by the policy
- access requests and approvals
- access rights and responsibilities
- change management processes for access control systems
- access privilege change criteria and authorizations for change
- access privilege database
- list of excessive or inappropriate access privileges
- list of access privileges to be deprovisioned
- process plan
- policies and procedures
- contracts with external entities

AM:GG2.GP7 Identify and Involve Relevant Stakeholders

Identify and involve the relevant stakeholders of the access management process as planned.

Elaboration:

Several AM-specific practices address the involvement of asset owners and custodians as key stakeholders in the access management process. For example, AM:SG1.SP1 describes the role of asset owners in assigning, approving, and revoking access privileges and the role of asset custodians in implementing access requests. AM:SG1.SP2 and AM:SG1.SP3 provide guidance on the role of asset owners in initiating, reviewing, and approving changes to access privileges and the role of asset custodians in maintaining access controls.

Subpractices

1. Identify process stakeholders and their appropriate involvement.

   Elaboration:

   Stakeholders of the plan include organizational staff who request, grant, or support the provision of access privileges to organizational assets.

   These are examples of stakeholders of the access management process:

   - asset owners and custodians
   - service owners
   - organizational unit and line of business managers responsible for assets
   - owners and sponsors of identities requiring access
   - staff responsible for developing, implementing, and managing an internal control system for assets
   - external entities responsible for making access requests and managing access to assets
   - human resources and legal departments as advisors on changes to access privileges
   - internal and external auditors

   Stakeholders are involved in various tasks in the access management process, such as

   - planning for the process
   - reviewing, initiating, approving, and revoking access requests and privileges
   - translating access requests/privileges to access controls
   - reconciling access privileges with roles, responsibilities, and identities
   - identifying and correcting inappropriate levels of access privileges
   - reviewing and appraising the effectiveness of process activities
   - resolving issues in the process

2. Identify these stakeholders to planners and those responsible for process performance.

3. Involve relevant stakeholders in the process as planned.

AM:GG2.GP8 Measure and Control the Process

Measure and control the access management process against the plan for performing the process and take appropriate corrective action.

Refer to the Monitoring process area for more information about the collection, organization, and distribution of data that may be useful for monitoring and controlling processes.

Refer to the Measurement and Analysis process area for more information about establishing process metrics and measurement.

Refer to the Enterprise Focus process area for more information about providing process information to managers, identifying issues, and determining appropriate corrective actions.

Subpractices

1. Measure actual performance against the plan for performing the process.

2. Review accomplishments and results of the process against the plan for performing the process.

   Elaboration:

   These are examples of metrics for the access management process:

   - percentage of asset owners participating in establishing and maintaining access privileges for the assets that they own
   - percentage of access requests that adhere to the access control policy
   - percentage of access acknowledgment forms that have been fully executed
   - percentage of access requests denied (based on policy)
   - percentage of approved access requests pending implementation beyond schedule
   - number of duplicate access requests
   - percentage of unapproved access requests that result in allowing access privileges (This should be zero.)
   - percentage of access requests that do not reflect the requestor’s role or job responsibilities (inadequate, excessive)
   - percentage of access privileges that are determined to be excessive or inappropriate based on the identity’s role or job responsibilities
   - elapsed time since access privileges were reviewed to ensure they reflect privileges assigned by the asset owner
   - rate of requests to change access privileges
   - percentage of access privilege change requests approved/denied
   - percentage of corrective actions to address excessive or inappropriate levels of access privileges pending beyond schedule
   - elapsed time from a change in access privileges requiring deprovisioning to the actual deprovisioning (mean, median)
   - number of risks related to inappropriate or excessive levels of access privileges that have been referred to the risk management process

3. Review activities, status, and results of the process with the immediate level of managers responsible for the process and identify issues.

   Elaboration:

   Periodic reviews of the access management process are needed to ensure that

   - policies are in place for managing access privileges

- ownership and custodianship over assets and access privileges for assets are established and documented access requests are submitted and approved according to policy
- change control processes are operating appropriately to ensure changes to access privileges are made and documented in a timely manner
- access privileges are periodically reconciled with roles, responsibilities, and identities
- access privilege inconsistencies are identified and corrected in a timely manner
- access privileges are deprovisioned when they are no longer valid or necessary
- status reports are provided to appropriate stakeholders in a timely manner
- unresolved issues surrounding inappropriate or excessive access privileges are referred to the risk management process when necessary
- actions requiring management involvement are elevated in a timely manner
- the performance of process activities is being monitored and regularly reported
- key measures are within acceptable ranges as demonstrated in governance dashboards or scorecards and financial reports
- administrative, technical, and physical controls are operating as intended
- internal controls are meeting the stated intent of the resilience requirements
- actions resulting from internal and external audits are being closed in a timely manner

4. Identify and evaluate the effects of significant deviations from the plan for performing the process.

   Elaboration:

   Deviations from the access management plan may occur when access requestors and asset owners fail to follow organizational policies regarding access request and approval. Significant deviations typically occur when changes in the operational environment and user community are not reflected in the current level of access privileges permitted. These deviations may permit unauthorized or inadvertent access to assets that can affect operational resilience.

5. Identify problems in the plan for performing and executing the process.
6. Take corrective action when requirements and objectives are not being satisfied, when issues are identified, or when progress differs significantly from the plan for performing the process.
7. Track corrective action to closure.

AM:GG2.GP9 Objectively Evaluate Adherence

Objectively evaluate adherence of the access management process against its process description, standards, and procedures, and address non-compliance.

Elaboration:

These are examples of activities to be reviewed:

- access request and approval process
- making changes to existing access privileges

- the alignment of stakeholder requirements with process plans
- assignment of responsibility, accountability, and authority for process activities
- determining the adequacy of process reports and reviews in informing decision makers regarding the performance of operational resilience management activities and the need to take corrective action, if any
- verification of process controls, including identifying and correcting excessive or inappropriate levels of access
- use of process work products for improving strategies to protect and sustain assets and services

These are examples of work products to be reviewed:

- access control policy and policy exceptions and waivers
- access privilege requests
- access privilege database
- access privilege change criteria
- action plans (for addressing inconsistencies)
- process plan and policies
- access privilege issues that have been referred to the risk management process
- process methods, techniques, and tools
- metrics for the process *(Refer to AM:GG2.GP8 subpractice 2.)*
- contracts with external entities

AM:GG2.GP10 Review Status with Higher Level Managers

Review the activities, status, and results of the access management process with higher level managers and resolve issues.

Refer to the Enterprise Focus process area for more information about providing sponsorship and oversight to the operational resilience management system.

AM:GG3 Institutionalize a Defined Process

Access management is institutionalized as a defined process.

AM:GG3.GP1 Establish a Defined Process

Establish and maintain the description of a defined access management process.

Establishing and tailoring process assets, including standard processes, are addressed in the Organizational Process Definition process area.

Establishing process needs and objectives and selecting, improving, and deploying process assets, including standard processes, are addressed in the Organizational Process Focus process area.

Subpractices

1. Select from the organization’s set of standard processes those processes that cover the access management process and best meet the needs of the organizational unit or line of business.
2. Establish the defined process by tailoring the selected processes according to the organization’s tailoring guidelines.
3. Ensure that the organization’s process objectives are appropriately addressed in the defined process, and ensure that process governance extends to the tailored processes.
4. Document the defined process and the records of the tailoring.
5. Revise the description of the defined process as necessary.

AM:GG3.GP2 Collect Improvement Information

Collect access management work products, measures, measurement results, and improvement information derived from planning and performing the process to support future use and improvement of the organization’s processes and process assets.

Elaboration:

These are examples of improvement work products and information:

- access requests
- approval of access requests
- issues related to change control on access privileges
- inconsistencies in levels of access privileges
- exceptions and waivers permitted to process policies
- metrics and measurements of the viability of the process *(Refer to AM:GG2.GP8 subpractice 2.)*
- changes and trends in operating conditions, risk conditions, and the risk environment that affect process results
- lessons learned in post-event review of incidents and disruptions in continuity
- process lessons learned that can be applied to improve operational resilience management performance, such as excessive or inappropriate access privileges and difficulties in assigning and executing asset ownership and custodianship responsibilities
- the level to which the status of the asset privileges is current, by asset type, asset owner, or other meaningful categorization schemes
- reports on the effectiveness and weaknesses of controls
- asset privilege corrective action plans that are not executed and the risks associated with them
- resilience requirements that are not being satisfied or are being exceeded

Establishing the measurement repository and process asset library is addressed in the Organizational Process Definition process area. Updating the measurement repository and process asset library as part of process *improvement and deployment is addressed in the Organizational Process Focus process area.*

Subpractices

1. Store process and work product measures in the organization’s measurement repository.
2. Submit documentation for inclusion in the organization’s process asset library.
3. Document lessons learned from the process for inclusion in the organization’s process asset library.
4. Propose improvements to the organizational process assets.