Software Engineering Institute

CERT® Resilience Management Model, Version 1.2

Identity Management (ID)

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.

DM-0003234

IDENTITY MANAGEMENT

Operations

Purpose

The purpose of Identity Management is to create, maintain, and deactivate identities that may need some level of trusted access to organizational assets and to manage identities' associated attributes.

Introductory Notes

Identity management is a process that addresses the life cycle of identities for objects and entities (systems, devices, or other processes) and for persons who need some level of trusted access to organizational assets (information; systems, servers, and networks; and facilities).

In identity management, identities for persons, objects, and entities are created so that they are made known to the organization and can be managed throughout their useful life. In the case of persons, these identities typically represent users of information, systems, and facilities who have unique identifying names (such as a user ID) and for whom information is known about their job roles and responsibilities in the organization. The creation of an identity is a means for profiling the person, object, or entity such that the identity retains a particular set of specific information (often referred to as the identity's DNA) as it traverses the organization and is provided different levels of trusted access to diverse organizational assets. This concept may even extend beyond the organization's borders. For example, a particular person, object, or entity may have more than one identity across different organizations that can be accumulated into a single identity (through a process called "federation").

The importance of establishing identities and understanding their DNA is so that they can be assigned access to organizational assets (through a process called "provisioning") and so that this access can be managed as the operational environment changes. This is tremendously important to managing operational resilience in that unauthorized or unintended access to organizational assets may result in unwanted outcomes such as

- disclosure of information (resulting in violations of privacy and confidentiality requirements)
- unauthorized use of systems and servers (to carry out fraudulent activities)
- unauthorized entry to secured facilities (which could affect the life, safety, and health of staff and customers)
- destruction or loss of vital information and systems that the organization relies upon day-to-day to carry out its strategic objectives

Because the operating environment is complex and the persons, objects, and entities that need access to organizational assets are ever-changing, the organization must actively manage the population of identities to ensure that it is valid. This is a challenging task that requires coordination and cooperation between the areas of the organization where identities

are created and managed (for example, in the IT department) and other departments such as human resources (where changes to the community of users are detected) and legal (where new business partners and vendors may have contractual agreements that require access to or ownership of assets).

Roles and responsibilities are linked to an organizational identity; that is, what a person or object has responsibility for in the organization (the person or object's role) determines the type and extent of access that is provided. Some roles are trusted—extraordinary access to organizational access is provided as a necessity for performing a distinct (and sometimes unique) job function. The role is associated with specific access privileges and restrictions that are imposed on the identity when access is provisioned.

Identities must be deprovisioned—that is, when the person, object, or entity ceases to exist in the organization, the identity is eliminated, and by reference all of its access privileges and restrictions are eliminated as well. The failure to deprovision an identity can result in significant operational risk to an organization because it may provide an identity to which an unauthorized (and perhaps unknown) person, object, or entity can associate. If this occurs and requisite access privileges have not been terminated, the identity can be stolen and provided by default with all of the existing privileges.

Identity management is often seen as a technical construct. This is because many of the processes for managing identities are operationalized as software packages and focus on electronic access to intangible assets such as information or to technical assets such as software, systems, hardware, and networks. However, in a broad sense, identity management is about establishing the existence of a person, object, or entity in the organization to which one or more access privileges can be assigned. These privileges can be electronic or physical (such as when providing access privileges to technology and facility assets). In some cases, identities may be established without any access privileges being provided.

To properly manage organizational identities, the organization must have processes to establish identities, deprovision identities, and manage changes that occur in the population of identities based on changes in the operating environment. Identities must be described in sufficient detail so that their attributes, including their roles and responsibilities, are clear and can be used as the basis for determining the appropriateness of assigning access privileges and restrictions.

Identity management and the management of access privileges are tightly coupled but distinct activities. An identity must exist to describe a particular role or responsibility in the organization. Access privileges are provided to the identity by virtue of its role. While connected, each of these activities represents a distinct aspect of access control and management that must be mastered to ensure that only authorized staff have access to organizational assets based on their need.

Related Process Areas

Access control and management are addressed in the Access Management process area.

Risks related to inconsistencies between identities and the persons, objects, and entities they represent are addressed in the Risk Management process area.

Summary of Specific Goals and Practices

Goals	Practices
ID:SG1 Establish Identities	ID:SG1.SP1 Create Identities
	ID:SG1.SP2 Establish Identity Community
	ID:SG1.SP3 Assign Roles to Identities
ID:SG2 Manage Identities	ID:SG2.SP1 Monitor and Manage Identity Changes
	ID:SG2.SP2 Periodically Review and Maintain Identities
	ID:SG2.SP3 Correct Inconsistencies
	ID:SG2.SP4 Deprovision Identities

Specific Practices by Goal

ID:SG1 Establish Identities

Identities are created to represent persons, objects, and entities that require access to organizational assets.

An identity documents the existence of a person, object, or entity that requires access to organizational assets such as information, technology, and facilities to fulfill its role in executing services. An identity most often represents a person (often referred to as a "user") but can be as diverse as a software application or system or other technology (such as a fax machine or process control device) that requires access to organizational information or systems. Persons, objects, and entities are usually internal to the organization (i.e., employed or controlled directly by the organization) but may be external (provided access to organizational assets in order to provide support services).

Managing the identities in an organization requires that the persons, objects, and entities be identified, profiled, and registered (through an identity profile) and that the organization establish a baseline identity community from which to perform identity-related activities.

ID:SG1.SP1 Create Identities

Persons, objects, and entities that require access to organizational assets are registered and profiled.

To become part of the organizational "community," identities must be registered and profiled. In essence, registration makes an identity "known" to the organization as a person, object, or entity that may require access to organizational assets and that may have to be authenticated and authorized to use access privileges.

The creation or registration of identities involves identifying the person, object, or entity and documenting detailed information about its role and position in the organization (or in an external organization, if applicable). The information that defines an identity is typically referred to as the identity's "DNA" because it is retained by the identity regardless of where it exists inside of or external to the organization. From an organizational perspective, the process of registration may occur when a new employee is hired by the organization and the person's role and job responsibilities are defined based on business requirements. However, it could also occur when an existing employee has a change in job responsibilities that would

require registration as an authorized user of organizational assets. Because the organizational environment is constantly changing, registration is an ongoing organizational activity that requires continuous processes.

Registration is performed for persons, objects, and entities that are internal and external to the organization. Thus, a vendor, agency, or business partner may be registered as an identity by the organization, as could a system or process from an external organization.

The typical vehicle for documenting the organization's identities is the identity profile. The profile contains all of the relevant information necessary to describe the unique attributes, roles, and responsibilities of the associated person, object, or entity. The identity profile is generally initiated and approved by an organizational unit or line of business to which the person belongs and where decisions about use of organizational assets can be made. In the case of objects and entities such as systems and processes, the organizational unit or line of business that "owns" the relationship essentially sponsors the identity creation and registration with the owner of the systems and processes that have to be registered.

Once established, an identity is the basis for assigning roles and access privileges in the organization. *(The association of privileges to identities and the ongoing management of privileges are addressed in the Access Management process area.)*

Typical work products

1. Justification for creation of identity
2. Identity profile

Subpractices

1. Establish an identity profile for persons, objects, and entities.

   Typically, the catalyst for the creation of an identity profile is a documented need for access to one or more organizational assets. The need may be established in advance of creating the profile (i.e., before a new employee begins employment) or concurrently with an access request to use an organizational asset. Not all persons, objects, and entities known to the organization will have an identity profile.

   An identity should have a sponsor—an organizational entity or person who is requesting the creation of the identity and agreeing to own the identity profile. The creation of an identity should be based on need and should be justified and authorized by the sponsor.

   The identity profile is the physical instantiation of an identity. The profile should include information such as

   - the name of the sponsor of the profile (This person has responsibility for approving subsequent actions to the profile.)
   - the person, object, or entity's name, location, department, and direct supervisor
   - other HR information (address, phone, etc.) if appropriate
   - a unique identifier for the identity (such as a user ID)
   - the identity's job responsibilities and position in the organizational structure

- the "roles" associated with the identity *(See ID:SG1.SP3.)*
- additional identity information such as "organization" if the identity is external to the organization
- any account groups that the identity may belong to (for example, accounts payable or engineering)
- the owner of an object or entity (if the identity profile is for an object or entity such as a system or business process)
- profile expiration or termination (if pre-established)
- special credentials of the person, object, or entity that would be needed to determine authorization and/or authentication for access to an organizational asset
- special restrictions on the person, object, or entity (such as work visa information)

ID:SG1.SP2 Establish Identity Community

The identity community is established and documented.

The identity community can be defined as the collection of the organization's identity profiles. The identity community defines the baseline population of persons, objects, and entities—internal and external to the organization—that could be or are authorized to access and use organizational assets such as information, technology, and facilities commensurate with their job responsibilities and roles. (In some cases, however, an identity may be established but have no access privileges associated with it.) Establishing the identity community is a foundational activity for protecting organization assets, managing changes to identities, and managing access privileges *(as described in the Access Management process area)*.

The organization must implement processes to collect and organize identities in a manner that defines and bounds the community of persons, objects, and entities. These processes establish a

- single, consistent source of information about identities and their range of influence and access
- baseline from which changes to identities can be monitored, identified, and managed
- scope for access control monitoring and analysis to identify unnecessary identities as well as to review access privileges and bring them into alignment with business and resilience requirements
- basis for the federation of identities (the process of aggregating the identity of a person, object, or entity across organizational units, organizations, systems, or other domains where it has multiple identities)

The degree to which the identity community is reflective of the current level of access provided to organizational assets is important in controlling access and ensuring that it does not result in additional vulnerabilities to high-value assets.

Typical work products

1. Identity repository

Subpractices

1. Create and maintain an identity repository.
2. Deposit identity profiles into the identity repository as they are created.
3. Establish access controls to ensure protection of identity information.

   Information contained on identity profiles can be considered sensitive and may have to be protected for privacy concerns under certain regulations and laws. In some cases, information such as Social Security number, date of birth, work visa information, and level of clearance may be included in the profile. This information, if subjected to unauthorized access, may not only subject the organization to potential fines and legal penalties but also expose the owner of the identity to possible identity theft.

ID:SG1.SP3 Assign Roles to Identities

Organizational roles are established and associated with identities.

Roles define a particular function that is associated with an identity. People, in particular, typically have many different roles in the organization that align with their job responsibilities. For example, a person may concurrently

- serve as the administrator over a payroll system
- be an authorized user of organizational facilities such as the data center or the call center
- be a reviewer of medical records or staff files
- be authorized to approve the payment of expenses

Roles are different from job responsibilities. Job responsibilities define what the person (or in some cases, object or entity) is bound to accomplish as a condition of employment. Roles describe the various positions that must be taken to carry out the job responsibilities. In some cases, roles are generic (commonly seen across all persons, objects, and entities), but others are trusted and specific (attributable only to a limited number of persons, objects, and entities). An identity will typically have more than one role assigned to it based on job responsibilities and the expected behaviors of the identity.

From a practical standpoint, roles are more easily defined for objects and entities such as systems and processes. For example, the role of a system may be to acquire information from another system on a nightly basis to facilitate reconciliation. When applied to people, roles become more extensive because staff members typically perform many different roles in carrying out their job responsibilities.

The establishment of roles is important because they establish the foundation for the assignment and association of access privileges to organizational assets. Particularly with people, access privileges are assigned to roles in an identity to avoid blanket assignments of access to assets based on criteria such as level and pay grade. (For example, a higher level manager who has responsibility for the department that manages the payroll system may have no justifiable reason to inquire on a staff member's payroll records.)

Roles must be developed and assigned to identities based on the knowledge and experience of business owners and the owners of organizational assets. For example, if a role calls for access to confidential medical records, there must be a justifiable business purpose for the access, and the owner of the medical records must sponsor the creation of and approve the role for the particular identity. In operation, because roles are usually tied to access requests, roles may not be assigned to identities until access has been requested. In addition, because roles have varying degrees of trust and responsibility, a single identity may possess many roles that exhibit the entire range of trust and responsibility.

Typical work products

1. Identity roles
2. Authorization for assignment of roles
3. Justification for assignment of roles
4. Updated identity profile

Subpractices

1. Develop, authorize, and justify roles.

   Line of business and organizational unit managers, asset owners, and human resources staff should be involved in the process of developing and assigning roles, including providing approval for the creation of a role and the association of the role with an identity. In some cases, the role created will be identical to a role established in an application system or other technology (such as a physical access control system), and in other cases, the role will be more descriptive of the identity's position and job responsibilities.

   The roles developed should be authorized and justified by the sponsors of the identities.

2. Assign roles to identities.

   Roles may be established at the time of creation of the identity profile or after it has been created.

ID:SG2 Manage Identities

Identities are managed to ensure they reflect the current environment of associated persons, objects, and entities.

Identities that have been registered represent the pool of persons, objects, and entities that can have access to high-value organizational assets. Unfortunately, these persons, objects, and entities are not a static group—changes in employment, business partnerships and relationships, and services bring about changes to the organization's pool of identities that must be managed on a daily basis.

The organization must be able to monitor for changes and ensure that identity profiles accurately represent the current pool of persons, objects, and entities in the organization. When misalignment occurs, the organization is potentially at risk because identities exist without corresponding persons, objects, or entities associated with them, possibly resulting in unauthorized or unintended access to organizational assets. When

identities do not have associated objects, the organization must act to deprovision these identities to reduce potential effects on operational resilience.

ID:SG2.SP1 Monitor and Manage Identity Changes

Changes to identities are monitored for and managed.

The pool of identities in an organization is dynamic—considering people alone, employees are hired, reassigned, transferred, and terminated on nearly a daily basis. The dynamic nature of the pool of identities is dictated by the almost constant change in an organization's business requirements and objectives as it adjusts to changing operational demands and risk environments. Changes in the environment must be accurately reflected in the inventory of identity profiles in a timely manner. Otherwise, the inventory will not reflect the current authorized level of access to organizational assets and cannot be relied upon as the baseline for managing protection of these assets.

Effective change management of the identity community requires organizational processes for monitoring the environment and identifying the addition and deletion of identities. Changes to identities—typically to the attributes and the roles—must also be monitored and managed. The organization must establish the criteria that indicate changes in the identity community and apply these criteria consistently throughout the enterprise.

This activity must also expand outside of the organization's boundaries to external suppliers and other business partners that have been provisioned as an identity by the organization and have been extended access rights to the organization's assets. Thus, the environment that must be monitored for changes can be vast and requires significant attention to reflect the actual and current pool of identities that are authorized to access and affect organizational assets. In addition, the identity profiles of current users should be updated accordingly.

Typical work products

1. Identity change criteria

Subpractices

1. Establish organizational criteria that may signify changes in the identity community.

   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 associated persons, objects, and entities.

   These are examples of conditions that signal a change in the identity community:

   - the addition of new employees (through notification by human resources or other hiring and benefits organizations)
   - changes in user responsibilities due to
     - transfers to different organizational units or departments
     - promotion or demotion
     - changes in job descriptions

  - changes in organizational structures
  - changes in structure of services
  - merger with or acquisition of other organizations
- termination of job responsibilities or employment
- addition, changes to, or deletion of supplier agreements and relationships (which may involve persons or systems and processes that have registered identities)
- addition, changes to, or termination of other business partnerships

2. Monitor for and manage changes to the identity community.

   Because changes occur constantly, inconsistency between the identity community and associated persons, objects, and entities can occur regularly. The organization should have processes to monitor for and manage changes so that inconsistencies are kept to a manageable minimum and do not pose risk to the organization. The termination of need for an identity in the organization is the most typical case that causes misalignment. As employees leave the organization, this is often not reflected in the active community of identities in a timely manner. In addition, as changes are made to systems and process control devices by business partners, the need for an organizational identity may expire but not be immediately known by the organization. These situations must be identified and monitored (as should those characterized in the organization's change criteria) so that timely identification of inconsistencies can occur.

   One means that the organization can use to proactively manage these issues is to place time restrictions on identities so that they expire automatically, particularly if they are tied through technical means to access rights on systems, facilities, and information assets.

ID:SG2.SP2 Periodically Review and Maintain Identities

Periodic review is performed to identify identities that are invalid.

Periodic review of identities is a detective and compensating control that can help the organization to keep the identity community viable and accurate. The periodic review should be performed by the organization with the intent of identifying identities that are no longer valid, are duplicated, or that have changed in some way but have not been detected by the organization's change management process *(as described in ID:SG2.SP1)*.

Allowing identities that are invalid or duplicated can have dire organizational consequences, particularly if these identities have access privileges associated with them. This can result in unauthorized

- use and modification of information
- use of systems and technology
- entry to and use of facilities

In addition to identifying invalid or duplicated identities, identity review may also uncover identities with invalid roles or responsibilities to which access privileges have been provisioned. These issues must also be uncovered during regular review and corrected in a timely manner.

Typical work products

1. Guidelines and timetables for identity review

2. List of inaccurate identity profiles
3. List of vacant or invalid identity profiles
4. List of redundant identity profiles
5. Documentation of actions proposed and actions taken

Subpractices

1. Establish a regular review cycle and process.

   Because of the potential risks of invalid or duplicate identities, the organization should establish a periodic review process to ensure alignment. The review cycle should consider the potential risks of unassigned identities as input to the time interval for performing this review. If excessive levels of invalid or duplicate identities are being detected on review, the review cycle should be appropriately adjusted.

2. Perform review of the identity community.

   Inconsistencies between the identity community and active persons, objects, and entities may allow unauthorized access to organizational assets. These inconsistencies must be identified on a regular and timely basis so that actions can be taken to limit potential misuse. The types of inconsistencies that may be identified include identity profiles that

   - do not reflect the current status, attributes, and roles of the associated person, object, or entity
   - are not associated with a valid or current person, object, or entity
   - are duplicative (more than one identity profile associated with a single person, object, or entity)
   - are being shared by more than one person, object, or entity

3. Identify inconsistencies in the identity community.

   Inconsistencies should be documented, as well as the actions that should be taken to eliminate or address them.

ID:SG2.SP3 Correct Inconsistencies

Inconsistencies between the identity community and the persons, objects, and entities they represent are corrected.

Inconsistencies between the identity community and the active, authorized community of associated persons, objects, and entities must be corrected in a timely manner to prevent vulnerabilities and risks that result from potential unauthorized use. While the potential for misuse is primarily concentrated on access privileges, the identity profile is the basis for this access and can be an effective first point of action. (This is particularly true in organizations where the identity profile is used to control all access rights.)

Correcting inconsistencies typically requires the organization to take one or more actions:

- Create new identity profiles. (In some cases, new identity profiles must be created when one or more persons have been sharing a single identity profile. This must be authorized, however, by relevant line of

business and organizational unit managers, asset owners, and human resources staff.)

- Make changes to the existing identity profile (to account for changing aptitudes or roles).
- Eliminate or deprovision duplicate identity profiles.
- Deprovision identity profiles that do not represent an active person, object, or entity.
- Federate duplicated identity.

This correction process also importantly extends to any persons, objects, or entities outside of the organization such as suppliers and business partners.

Correcting inconsistencies may also require the involvement of business owners and sponsors of identity profiles. For example, the deprovisioning of an identity should be acknowledged and approved by business owners, as should any changes to an active identity profile. *Deprovisioning of identity profiles is addressed in ID:SG2.SP4*.

Typical work products

1. Written authorization for changes
2. Justification for forgoing corrective action
3. Correction status

Subpractices

1. Develop corrective actions to address inconsistencies in identity profiles.

   This may require detailed involvement of business units and owners who sponsored the creation of identity profiles.

2. Correct identity profiles as required.

   Corrections should be made only on the authorization and written acknowledgment of business units and owners of identity profiles.

3. Document disposition for inconsistencies that will not result in changes or corrections.

   In some cases, the organization may determine that changes are not required or warranted. This may pose additional risk to the organization that may have to be addressed. These risks should be referred to the organization's risk management process and should be fully acknowledged by business units, owners, or other sponsors of created identities. The decision to not correct inconsistencies should be documented and approved.

   The management of risks is addressed in the Risk Management process area.

4. Update status of corrective actions.

   The organization should perform status checks on all inconsistencies identified and ensure that a proper disposition—even if no action is taken—is provided for each.

ID:SG2.SP4 Deprovision Identities

Identities for which need has expired or has been eliminated are deprovisioned.

Deprovisioning is a process of deactivating or eliminating an identity (i.e., discarding or destroying the identity profile) as well as all of the privileges and restrictions associated with the identity. If the associated persons, objects, or entities no longer exist, then the identity should be deprovisioned.

Deprovisioning may occur as a result of the regular process of hiring and terminating staff. Human resources departments often feed hiring and termination information to those who are responsible for maintaining the organization's identity repositories as a catalyst for timely and effective creation and deprovisioning of identities. However, deprovisioning may be the result of corrective actions taken to remedy inconsistencies in the identity community. The organization must have processes for regular deprovisioning, particularly with respect to staff.

The elimination or deactivation of an identity also has implications for access privileges. The primary reason for deprovisioning is to prevent unauthorized or accidental access to organizational assets. Thus, when this process is not automated, the act of deprovisioning an identity may require an extensive identification and elimination of associated access privileges. *(The deprovisioning of access privileges associated with an identity's roles is addressed in the Access Management process area.)*

As with all identity management activities, business owners and units should be involved in the deprovisioning process.

Typical work products

1. Written authorization for deprovisioning
2. Deprovisioned identity profiles
3. Updated identity repository

Subpractices

1. Obtain written approval from line of business and organizational unit managers, asset owners, and human resources staff for deprovisioning identities.

   Line of business and organizational unit managers, asset owners, and human resources staff may recommend whether the identity should be simply deactivated (indicating that it may be used in the future) or eliminated (destroying the identity and requiring re-creation if the need arises in the future).

2. Identify and trace access privileges associated with the identity's roles.

   The deprovisioning of the identity profile should ensure that all relevant access privileges are eliminated as well. Depending on how the organization manages identity profiles, this may be a simple or extensive activity.

3. Deprovision identities as required.

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 Identity Management process area.

ID:GG1 Achieve Specific Goals

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

ID:GG1.GP1 Perform Specific Practices

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

Elaboration:

Specific practices ID:SG1.SP1 through ID:SG2.SP4 are performed to achieve the goals of the identity management process.

ID:GG2 Institutionalize a Managed Process

Identity management is institutionalized as a managed process.

ID:GG2.GP1 Establish Process Governance

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

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

Subpractices

1. Establish governance over process activities.

   Elaboration:

   Governance over the identity management process may be exhibited by

   - developing and publicizing higher level managers' objectives and requirements for the process
   - sponsoring policies, procedures, standards, and guidelines for the process
   - 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
   - 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 prioritizing process requirements and improving the process
- providing input on identifying, assessing, and managing operational risks related to the process, including guidance for resolving identity inconsistencies and other anomalies
- 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 identity management policy should address

- responsibility, authority, and ownership for performing process activities, including line of business and organizational unit managers, asset owners, and human resources staff approval of roles and associated identities
- procedures, standards, and guidelines for
  - approving and provisioning identity profiles
  - approving and provisioning identity profiles that provide trusted levels of access (including special credentials)
  - approving and provisioning identity profiles that exclude levels of access (including special restrictions)
  - assigning roles to identities
  - assigning access privileges to roles
  - managing changes to identity profiles
  - identifying and correcting inconsistencies between identity profiles and the persons, objects, and entities they represent
  - deprovisioning identities
- methods for measuring adherence to policy, exceptions granted, and policy violations

ID:GG2.GP2 Plan the Process

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

Elaboration:

For practical purposes, identity management may be a highly centralized activity that relies on a set of designated administrators who have the requisite authority to provide identity management of guest accounts and group management in their geography or for a set of specific assets. For this reason, the organization may have a plan that covers the general management of identity profiles and also specific plans that address the special considerations unique to each type of identity or asset. Identity management may also be tightly coupled with the access management processes, tools, techniques, and methods.

Subpractices

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

Elaboration:

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

ID:GG2.GP3 Provide Resources

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

Subpractices

1. Staff the process.

   Elaboration:

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

   - staff responsible for
     - establishing, registering, and profiling identities for persons, objects, and internal and external entities, possibly including organizational unit and line of business managers, asset owners, and human resources
     - creating and maintaining an identity repository
     - authorizing, justifying, and assigning roles to identities
     - ensuring that identity information is appropriately protected to meet privacy and security requirements
     - reviewing, monitoring, and managing changes to identities, including deprovisioning
   - physical security staff responsible for issuing and monitoring the use of identity badges or other types of physical identity tokens
   - information technology staff responsible for implementing identity controls using systems and other technologies
   - 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 identity 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 to implement and manage the life cycle of identities for persons, objects, and entities that need some level of trusted access to organizational assets.

ID:GG2.GP3 subpractice 3 tools, techniques, and methods do not include those necessary to implement and manage administrative (policy), technical, or physical access controls. *(Refer to the Access Management process area for more information about this aspect.)*

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

- tools, techniques, and methods for
  - creating identity profiles and an identity repository
  - associating specific access privileges and restrictions with a given role
  - aggregating multiple identities of a person, object, or entity (federation)
  - managing changes to identities
  - reviewing identities and correcting inconsistencies between stored identities and the people, objects, and entities they represent
  - deprovisioning identities
- methods for developing role definitions and authorizing and justifying the assignment of roles to identities
- tools for tracking corrective actions to resolve identity inconsistencies 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.

ID:GG2.GP4 Assign Responsibility

Assign responsibility and authority for performing the identity 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 identity management process may be distributed across the organization and involve both organizational units and information technology. Identities can be internal or external to the organization. The creation and registration of identities may be triggered by the hiring of new staff, a change of responsibility for existing staff, or the addition of a new business partner or vendor that needs access to assets. Line of business and organizational unit managers (and specifically asset owners) are typically responsible for the authorization, justification, and approval processes that make up the identity profile,

while information technology and physical security staff are responsible for mapping the role to the requisite privileges and access to assets. Change management for identities is typically a shared responsibility among organizational units, information technology, and physical security because they must coordinate activities to ensure that privileges are granted to only credentialed entities.

ID:GG2.GP4 subpractice 1 does not specifically cover responsibility for the development and implementation of access controls for information, technology, or facilities. ID:GG2.GP4 subpractice 1 is limited to responsibility for creating, registering, and deprovisioning identities and managing changes to identities.

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 identity management tasks can be formalized by

- defining roles and responsibilities in the process plan
- including process tasks and responsibility for these tasks in specific job descriptions
- developing policy requiring line of business managers, project managers, asset owners, and human resources staff to participate in the justification, authorization, and approval of identities and associated roles for assets under their ownership
- developing policies requiring information technology and physical security staff to perform process tasks relative to manager and asset owner instructions
- including process tasks in staff performance management goals and objectives, with requisite measurement of progress against these 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.

ID:GG2.GP5 Train People

Train the people performing or supporting the identity 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 creating a skill set inventory, establishing a skill set baseline, identifying required skill sets, and measuring and addressing skill deficiencies.

Subpractices

1. Identify process skill needs.

   Elaboration:

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

   - knowledge of tools, techniques, and methods used to manage and maintain identities, including those necessary to perform the process using the selected methods, techniques, and tools identified in ID:GG2.GP3 subpractice 3
   - knowledge necessary to elicit and prioritize stakeholder requirements and needs and interpret them to develop effective requirements for the process
   - knowledge necessary to analyze and prioritize process requirements
   - knowledge necessary to associate identities with roles and assign appropriate access privileges based on these
   - knowledge necessary to manage identities in a manner appropriate for accessing each type of organizational asset (i.e., information; systems, servers, and networks; and facilities) by each type of identity (persons, objects, and entities)

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:

   - eliciting and capturing stakeholder identity management requirements
   - creating and registering identities, including federated identities
   - credentialing identities
   - assigning roles and access privileges to identities
   - managing changes to identities
   - deprovisioning identities
   - using controls to protect and secure identity profiles and repositories
   - working with external entities to establish their identities in accordance with policy
   - using process methods, tools, and techniques

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

ID:GG2.GP6 Control Work Products

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

Elaboration:

Tools, techniques, and methods should be employed to support the creation, provisioning, change management, and deprovisioning of identities and corresponding roles as a baseline

from which changes to identities can be monitored and managed. These tools may also be used as a basis for federation of identities.

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

- lists of internal and external stakeholders and a plan for their involvement
- identity profiles
- identity repositories
- identity roles and associated access privileges
- identity change criteria
- lists of identity profiles that are inaccurate or inconsistent, including required change management action
- deprovisioned identities
- process plan
- policies and procedures
- contracts with external entities

ID:GG2.GP7 Identify and Involve Relevant Stakeholders

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

Subpractices

1. Identify process stakeholders and their appropriate involvement.

   Elaboration:

   These are examples of stakeholders of the identity management process:

   - staff associated with each process requirement, object, profile, and asset
   - organizational unit and line of business managers who typically initiate and approve establishing and updating identities
   - business owners and owners of organizational assets, to ensure that roles and access privileges are appropriately assigned to identities and regularly reviewed and updated
   - new and existing staff who require a current identity profile
   - terminated staff whose identities are deprovisioned
   - human resources
   - legal counsel and staff
   - chief privacy officer or equivalent to ensure sensitive identity information is adequately protected
   - business partners, vendors, and outsourcers that require an identity to gain access
   - staff responsible for reviewing identities and updating identities
   - staff associated with each external entity that has an active identity
   - staff associated with the deprovisioning of identities
   - internal and external auditors

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

- establishing requirements for the process
- planning for the process
- making decisions about process scope and activities
- vetting and reviewing identity profiles, roles associated with profiles, and access privileges associated with roles
- reviewing and appraising the effectiveness of process activities
- resolving issues in the process and with identity inconsistencies, including reconciling and approving changes to identities
- federating identities
- deprovisioning identities

2. Communicate the list of stakeholders to planners and those responsible for process performance.
3. Involve relevant stakeholders in the process as planned.

ID:GG2.GP8 Measure and Control the Process

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

Elaboration:

Refer to the Monitoring process area for more information about the collection, organization, and distribution of data that may be useful for measuring 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 identity management process:

   - elapsed time from identity request to granting of identity credentials
   - percentage of identity requests denied (based on policy)
   - percentage of identity requests approved that, on further investigation, should have been denied based on, for example, a mismatch with designated roles
   - percentage of identity requests that duplicate previous or current requests
   - percentage of identities for which roles have been authorized and justified by identity owners
   - rate of change requests to current identity profiles

- number of inconsistencies between identity profiles and their associated persons, objects, and entities
- percentage of identity profiles that are inaccurate
- percentage of identity profiles that are vacant or invalid
- percentage of identity profiles that are redundant
- percentage of identity community inconsistencies for which corrective action is pending beyond schedule
- percentage of identities belonging to external entities
- percentage of deprovisioned identities whose deprovisioning is pending beyond schedule
- number of incidents involving the identity repository
- number of incidents involving the identity repository for which resolution is pending beyond schedule
- number of identity-related risks 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 identity management process are needed to ensure that

   - policies are in place to guide the process for managing identity profiles
   - identity requests are submitted and approved according to policy
   - changes to identities are made in a timely manner and documented
   - identity profiles are periodically reconciled
   - identity inconsistencies are identified and corrected in a timely manner
   - identities are deprovisioned in a timely manner
   - 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
   - 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:

   Discrepancies result when identities are created, changed, federated, or deprovisioned but not accurately reflected in the identity community, identity profiles, or the identity repository. Authorized access to assets and the services they support is based on accurate, up-to-date identities. To the extent that the identity management process results in an inaccurate definition of the identity community or population, the organization's overall ability to manage operational resilience is impeded.

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.

ID:GG2.GP9 Objectively Evaluate Adherence

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

Elaboration:

These are examples of activities to be reviewed:

- developing identity profiles
- identifying identity change criteria
- making changes to identity profiles and to the identity repository
- resolution of identity inconsistencies
- timeliness of identity deprovisioning
- the alignment of stakeholder requirements and needs with the process plan
- assignment of responsibility, accountability, and authority for process activities
- determination of 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 identity management data confidentiality, integrity, and availability controls
- use of process data to improve strategies for protecting and sustaining assets

These are examples of work products to be reviewed:

- identity profiles
- identity repository
- identity change control logs
- deprovisioned identities
- process plan and policies
- process scope and requirements
- process methods, techniques, and tools *(Refer to ID:GG2.GP3 subpractice 3.)*
- metrics for the process *(Refer to ID:GG2.GP9 subpractice 2.)*
- contracts with external entities

ID:GG2.GP10 Review Status with Higher Level Managers

Review the activities, status, and results of the identity 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.

ID:GG3 Institutionalize a Defined Process

Identity management is institutionalized as a defined process.

ID:GG3.GP1 Establish a Defined Process

Establish and maintain the description of a defined identity 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 identity management process and that 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 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.

ID:GG3.GP2 Collect Improvement Information

Collect identity 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:

- the current status of identity profiles
- the status of confidentiality, integrity, and availability for identity profiles and repositories, as determined by the results of integrity and security tests
- metrics and measurements of the viability of the process *(Refer to ID: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 poorly documented or inconsistent identities
- reports on the effectiveness and weaknesses of controls
- process requirements that are not being satisfied 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.