Software Engineering Institute

CERT® Resilience Management Model, Version 1.2

Technology Management (TM)

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/

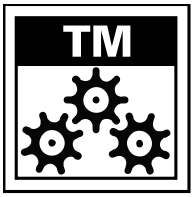
Carnegie Mellon

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

TECHNOLOGY MANAGEMENT

Operations



Purpose

The purpose of Technology Management is to establish and manage an appropriate level of controls related to the integrity and availability of technology assets to support the resilient operations of organizational services.

Introductory Notes

Technology is a pervasive organizational asset. Few organizational services are untouched by some aspect of technology—hardware, software, systems, tools, and infrastructure (such as networks) that support services. Technology assets directly support the automation (and efficiency) of services and are often inextricably tied to information assets because they provide the platforms on which information is stored, transported, or processed. For some organizations, technology is a prominent driver in accomplishing the mission and is considered a strategic element. Technology tends to be pervasive across all functions of the organization and therefore can be a significant contributor to strategic and competitive success.

From a broad perspective, technology describes any technology component or asset that supports or automates a service and facilitates its ability to accomplish its mission. Examples of technology assets include software, hardware, and firmware, including physical interconnections between these assets such as cabling. Technology has many layers, some of which are specific to a service (such as an application system) and others of which are shared by the organization (such as the enterprise-wide network infrastructure) to support more than one service. Organizations must describe technology assets sufficiently to facilitate development and satisfaction of resilience requirements. In some organizations, this may be at the application system level; in others, it might be more granular, such as at the server or personal computer level.

The Technology Management process area addresses the importance of technology assets in the operational resilience of services, as well as unique issues specific to technology such as integrity and availability management. In this process area, technology assets are prioritized according to their value in supporting high-value organizational services. Physical, technical, and administrative controls that keep technology assets viable and sustainable are selected, implemented, and managed, and the effectiveness of these controls is monitored. In addition, technology asset risks are identified and addressed in an attempt to prevent disruption where possible.

The integrity of technology assets is addressed through mastery of capabilities such as configuration, change, and release management. The availability of technology assets, critical for supporting the resilience of services, is established and managed by controlling the operational environment in which the assets operate, by performing regular maintenance on these assets, and by limiting the potential effects of interoperability issues. Because technology assets may extend outside of the physical and logical boundaries of the

organization, the organization must address the interaction with external entities that provide technology assets or support for technology assets to the organization.

Related Process Areas

The establishment and management of resilience requirements for technology assets are performed in the Resilience Requirements Development and Resilience Requirements Management process areas.

The identification, definition, management, and control of technology assets are addressed in the Asset Definition and Management process area.

The risk management cycle for technology assets is addressed in the Risk Management process area.

The management of the internal control system that ensures the protection of technology assets is addressed in the Controls Management process area.

The selection, implementation, and management of access controls for technology assets are performed in the Access Management process area.

The development of service continuity plans for technology assets is performed in the Service Continuity process area.

The establishment and management of relationships with external entities to ensure the resilience of services that are executed in facilities they own and operate are addressed in the External Dependencies Management process area.

Summary of Specific Goals and Practices

Goals	Practices
TM:SG1 Establish and Prioritize Technology Assets	TM:SG1.SP1 Prioritize Technology Assets
	TM:SG1.SP2 Establish Resilience-Focused Technology Assets
TM:SG2 Protect Technology Assets	TM:SG2.SP1 Assign Resilience Requirements to Technology Assets
	TM:SG2.SP2 Establish and Implement Controls
TM:SG3 Manage Technology Asset Risks	TM:SG3.SP1 Identify and Assess Technology Asset Risks
	TM:SG3.SP2 Address Technology Asset Risks
TM:SG4 Manage Technology Asset Integrity	TM:SG4.SP1 Control Access to Technology Assets
	TM:SG4.SP2 Perform Configuration Management
	TM:SG4.SP3 Perform Change Control and Management
	TM:SG4.SP4 Perform Release Management
TM:SG5 Manage Technology Asset Availability	TM:SG5.SP1 Perform Planning to Sustain Technology Assets
	TM:SG5.SP2 Manage Technology Asset Maintenance
	TM:SG5.SP3 Manage Technology Capacity
	TM:SG5.SP4 Manage Technology Interoperability

Specific Practices by Goal

TM:SG1 Establish and Prioritize Technology Assets

Technology assets are prioritized to ensure the resilience of the high-value services that they support.

In this goal, the organization establishes the subset of technology assets (from its technology asset inventory) on which it must focus operational resilience activities because of their importance to the sustained operation of essential services.

Prioritization of technology assets is a risk management activity. The organization establishes the technology assets that are of most value to providing business services and for which controls to protect and sustain them are required. Failure to prioritize technology assets may lead to inadequate operational resilience of high-value assets or excessive levels of operational resilience for non-high-value assets.

TM:SG1.SP1 Prioritize Technology Assets

Technology assets are prioritized relative to their importance in supporting the delivery of high-value services.

The prioritization of technology assets must be performed in order to ensure that the organization properly directs its operational resilience resources to the assets that most directly impact and contribute to services that support the organization's mission. These assets require the organization's direct attention because their interruption or disruption has the potential to cause significant organizational consequences, particularly because the health and viability of information assets are typically tied directly to the resilience of technology assets.

Technology asset prioritization is performed relative to related services—that is, technology assets associated with high-value services are those that must be most highly prioritized for operational resilience activities. The organization may use other criteria to establish high-priority technology assets, such as

- the relationship between the technology and the value of the information assets stored, transported, or processed by the technology
- technology assets such as networks that are considered to be foundational and are vital to supporting more than one organizational service
- proprietary technology assets provided by suppliers (such as application systems or specific types of hardware) that would materially affect the organization if the supplier is unreachable or drops support
- the degree to which the technology assets are "redundant"—that is, easily replaceable or able to be replicated if lost or destroyed
- technology assets that automate resilience controls (such as physical access systems) that are critical to sustaining operational resilience
- resilience technology assets that are specifically designated to support the organization's ability to support service continuity plans

Typically, the organization selects a subset of technology assets from its asset inventory; however, the organization could compile a list of high-value assets based on risk or other factors. However, failure to select assets from the organization's asset inventory poses additional risk that some high-value technology assets may never have been inventoried. *(The identification, definition, management, and control of technology assets are addressed in the Asset Definition and Management process area.)*

Typical work products

1. List of high-value technology assets

Subpractices

1. Compile a list of high-value technology assets from the organization's technology asset inventory.

   Technology assets that are essential to the successful operation of organizational services should be included on the list of technology assets. *(An inventory of high-value assets is established in practice ADM:SG1.SP1 in the Asset Definition and Management process area.)* This list may suffice for this subpractice or may be expanded if necessary.

   Technology includes the entire infrastructure necessary to design, manufacture, operate, maintain, and repair technological assets. These are examples of high-value technology assets:

   - software
   - hardware
   - firmware
   - network infrastructure, including cables and other types of interconnections
   - automated systems and applications
   - tools
   - telecommunications and utility services

2. Prioritize technology assets.

   The prioritization of technology assets is necessary to ensure the organization focuses on activities to protect and sustain the technology that is essential to the successful operation of organizational services.

   It must be considered that many high-value organizational services may rely upon shared technology assets such as email applications, web servers, or network infrastructure. The disruption or failure of these types of technology assets can cause cascading effects on many organizational services; therefore, they should be of higher priority in addressing operational resilience.

3. Periodically validate and update the list of high-value technology assets based on operational and organizational environment changes.

TM:SG1.SP2 Establish Resilience-Focused Technology Assets

Technology assets that specifically support execution of service continuity plans are identified and established.

Service continuity plans may rely heavily on technology assets for successful execution. These assets may be those that are in production or others that are designated for resilience purposes. For example, the organization may have spare servers or telecommunications bandwidth that can be called into service when primary technology assets fail or when service continuity plans require specific assets to execute recovery and restoration activities.

Resilience technology assets may be contracted for and provided by an external entity. For example, an organization may contract with an outside disaster recovery provider to provide access to servers and other technology assets to allow off-site recovery of application systems. In such arrangements, the technology assets involved are typically not owned by the organization, but they should still be included in the organization's list of resilience technology assets.

If the organization owns facilities that are specifically designated for backup and recovery, the technology assets that are contained in these facilities are typically not used in daily operations and are owned by the organization. These assets should also be included in the organization's list of resilience technology assets and protected accordingly.

The identification of resilience facilities that may in turn contain resilience technology assets is performed in the Environmental Control process area. There should be coordination between the facility and technology assets that are identified in this specific practice.

Typical work products

1. List of resilience technology assets.

Subpractices

1. Compile a list of resilience technology assets from the organization's asset inventory.

   These technology assets should include those that would be required for the successful execution of service continuity plans.

2. Periodically reconcile the list of resilience technology assets to the organization's service continuity plans and resilience strategies.

   These technology assets should also be reconciled to the resilience facilities identified in practice EC:SG1.SP2 in the Environmental Control process area.

TM:SG2 Protect Technology Assets

Administrative, technical, and physical controls for technology assets are identified, implemented, monitored, and managed.

Technology assets are pervasive across the organization. An organization may have hundreds or thousands of services that are supported or automated by technology

assets. As a complicating factor, many of these assets may not be owned by the organization because services often traverse organizational boundaries and are supported or operated by business partners and vendors. Thus, the organization may not have direct control or influence over the controls for protecting and sustaining these assets.

Because of their pervasiveness, a primary consideration for technology assets is availability. Keeping technology assets productive consumes a large amount of organizational effort because these assets are directly tied to mission success for services. In addition, the complexity of technology assets, particularly software and systems, means that the integrity of the assets is paramount. The integrity of technology assets is ensured by strong change and configuration processes and controls and the protection of technology assets from inappropriate or unauthorized access.

To protect technology assets, the organization should

- develop appropriate resilience requirements for the assets
- develop, implement, and manage an appropriate level of administrative, technical, and physical controls to manage the conditions that could cause disruption of the assets
- select and design controls based on the assets' resilience requirements and the range of conditions that require integrity of the asset configuration and availability of the assets to perform their intended functions
- monitor the effectiveness of these controls on a regular basis to ensure that they meet the technology assets' resilience requirements

TM:SG2.SP1 Assign Resilience Requirements to Technology Assets

Resilience requirements that have been defined are assigned to technology assets.

Resilience requirements form the basis for the actions that the organization takes to protect and sustain technology assets. These requirements are established commensurate with the value of the assets to services that they support. The resilience requirements for technology assets must be assigned to the assets so that the appropriate type and level of protective controls can be designed, implemented, and monitored to meet the requirements.

With technology assets, there may be instances of conflicting requirements because many of these assets are shared by more than one service and may be related to information assets that have specific data categorization or confidentiality requirements. These situations of shared requirements must be analyzed and considered when assigning resilience requirements to technology assets, with the intention of providing a baseline requirement that is sufficient to encompass the most stringent requirements.

Resilience requirements for technology assets are developed in the Resilience Requirements Development process area. However, technology asset resilience requirements may not be formally defined or they may be assumed to be the responsibility of the technology asset owner (if the

organization is not the owner). The assignment of these requirements is necessary as a foundational step for controls selection and management.

Typical work products

1. Technology asset resilience requirements

Subpractices

1. Assign resilience requirements to technology assets.

   Resilience requirements for technology assets must take into consideration the shared nature of the technology within the organization (since more than one service is likely to use common technology) and technology outside of the organization (such as an external service provider or co-location of communications equipment, which may have different resilience requirements).

2. Document the requirements (if they are currently not documented) and include them in the asset definition.

TM:SG2.SP2 Establish and Implement Controls

Administrative, technical, and physical controls that are required to meet the established resilience requirements are identified and implemented.

The organization must implement an internal control system that protects the continued operation of technology assets commensurate with their role in supporting organizational services. Controls are essentially the methods, policies, and procedures that the organization uses to provide an acceptable level of protection over high-value technology assets. Controls typically fall into three categories: administrative (or managerial), technical, and physical. All of these controls are necessary for technology assets because they come in so many different forms and are pervasive across the organization.

- Administrative controls ensure alignment to higher level managers' intentions and include such work products as governance, policy, monitoring, auditing, separation of duties, and the development and implementation of service continuity plans. Administrative controls provide guidance regarding who can access technology assets, make changes to their configuration, or establish timetables governing when they can be used and for what purpose.
- Technical controls are the technical manifestation of protection methods for technology assets. In essence, technology assets often act as technical controls, such as when a firewall is deployed to manage network traffic or when specialized software is used to manage access to information. The use of technical assets as protective controls is most often associated with security activities.
- Physical controls manage the physical access and modification of technology assets. These controls typically include separating software development environments from production environments, locking equipment room doors, and other physical barrier methods.

Operational resilience for technology assets involves a thorough consideration of a wide range of controls. These include not only physical and logical access controls but controls that address the integrity, availability, and operability of the technology in its environment and in environments out of the direct control of the organization. Regardless of location, resilience requirements are the responsibility of the technology asset owners and must be provided to the custodian of technology assets for implementation.

Typical work products

1. Technology asset administrative controls
2. Technology asset technical controls
3. Technology asset physical controls

Subpractices

1. Establish and implement administrative controls for technology assets.

   Administrative controls for technology assets include

   - policies that govern technology users' behavior with regard to information assets
   - standards on selection, interoperability, and integration of technology assets
   - standards for the configuration and change management of technology assets such as software or the baseline configuration footprint of hardware
   - policies for the proper disposition of technology assets
   - certification and accreditation of systems and applications
   - policies for the removal of technology assets from the workplace
   - staff hiring procedures, particularly with regard to access to confidential information or performance of maintenance on technology assets
   - training to ensure proper technology asset definition and handling *(See the Organizational Training and Awareness process area.)*
   - logging, monitoring, and auditing controls to detect and report unauthorized access and use of technology *(See the Monitoring process area.)*
   - governance over the proper use and distribution of technology and the protection of technology assets *(See the Enterprise Focus process area.)*
   - development, testing, and implementation of service continuity plans (including technology asset recovery and restoration and the assignment of technology assets to plans) (*See the Service Continuity process area.)*

2. Establish and implement technical controls for technology assets.

   Technical controls include such controls as

   - configuration and change management
   - software quality assurance
   - software escrow
   - file integrity auditing software
   - access control lists and related methodologies
   - automated backup, retention, and recovery of technology assets
   - modification controls that prevent unauthorized modification and that log and report modification actions by authorized individuals

3. Establish and implement physical controls for technology assets.

   Physical controls for protecting technology assets include such controls as

   - security guards, surveillance cameras, fences, locking equipment cabinets or rooms, and other physical security mechanisms
   - physical access controls on file rooms and work areas where paper and technology assets are stored
   - fire alarms and protection
   - water alarms and protection
   - electrical power conditioning
   - limited entry points to areas where technology is stored, transported, or processed

4. Establish and specify controls over the design, construction, and acquisition of technology assets.

   These controls ensure that the development and acquisition of software and systems or the development and acquisition of hardware are performed with consideration of the operational resilience of these assets. *(These activities and related practices are specifically addressed in the Resilient Technical Solution Engineering process area.)*

5. Monitor the effectiveness of administrative, technical, and physical controls, and identify deficiencies that must be resolved. *(See CTRL:SG4.SP1 in the Controls Management process area.)*

TM:SG3 Manage Technology Asset Risks

Operational risks to technology assets are identified and managed.

Risks to technology assets are managed by the application of risk management tools, techniques, and methods to those assets. Because of the pervasiveness of technology assets across the organization, their complex nature, and the various forms in which they can be found, there are many opportunities for technology assets to be threatened and for risk to be realized by the organization. Risks to technology assets can result in cascading consequences to the organization, including the disruption of high-value services due to the lack of technology usability and availability.

Technology assets are prone to specific types of operational risk, including the failure of systems and technology due to

- complexity due to poor design, failure to "build security in," poor requirements, and immature software and systems engineering processes
- poor configuration and change management, which increases exposure to vulnerabilities
- inadvertent and deliberate actions of people, particularly technology staff or external people such as hackers
- environmental conditions in places where technology assets are located

Because technology assets can often act as "containers" for information assets, risks to technology assets can also have a cascading effect on information assets. In addition, because technology assets "live" in facilities, risks to facilities must be examined to determine if they can affect technology assets.

The identification and response to risks to information are addressed in the Knowledge and Information Management process area. The identification and response to risks to facilities are addressed in the Environmental Control process area.

TM:SG3.SP1 Identify and Assess Technology Asset Risks

Risks to technology assets are identified and assessed.

Operational risks that can affect technology assets must be identified and addressed in order to actively manage the resilience of these assets and, more important, the resilience of services to which these assets are associated.

The identification of technology asset risks forms a baseline from which a continuous risk management process can be established and managed.

The subpractices included in this practice are generically addressed in goals RISK:SG3 and RISK:SG4 in the Risk Management process area.

Typical work products

1. Technology asset risk statements, with impact valuation
2. List of technology asset risks, with categorization and prioritization

Subpractices

1. Determine the scope of risk assessment for technology assets.

   Determining which technology assets to include in regular risk management activities depends on many factors, including the value of the assets to the organization, their resilience requirements, and the ownership and control of the specific technology.

2. Identify risks to technology assets.

   Identification of risks to technology assets is broad in scope because of the many types of technology assets. For example, operational risks to software assets may differ significantly from those that threaten hardware assets or networks. The type of technology asset and the environment in which the asset is operating will form a baseline scope for the identification of risk.

   Typically, operational risks for technology assets include such broad areas as

   - unauthorized access to and destruction of technology assets (including physical destruction of the assets or the manipulation of hardware or software configurations, rendering the assets unusable)
   - exerting unwanted control over the assets (such as with hacking or denial of service) that makes the assets unusable or unstable
   - poor design of technology assets that results in weaknesses that can be exploited
   - poor implementation or operational controls that reduce the reliability, availability, and ability to sustain the assets (including deficient change and configuration management processes)
   - physical and environmental conditions such as humidity, or exposure to natural conditions such as flood
   - inadvertent or accidental misuse related to poor administrative controls such as appropriate use policies

- inadvertent or deliberate actions of custodians (particularly external to the organization) who have been entrusted to protect technology assets

Operational risks should be identified in the context of type and physical location so that response actions are more focused and directed.

Risk statements should be developed for each identified risk. *(RISK:SG3.SP1 and RISK:SG3.SP2 provide additional information about identifying risks and developing risk statements.)*

3. Analyze risks to technology assets.
4. Categorize and prioritize risks to technology assets.

   This may require the organization to view each class of technology asset separately (i.e., risks to software, risks to systems, risks to hardware such as servers, etc.).

   RISK:SG4.SP2 provides additional information about risk categorization and prioritization.

5. Develop a risk disposition strategy for each technology asset risk.

   RISK:SG4.SP3 provides additional information about risk disposition.

6. Monitor the risk and the risk strategy on a regular basis to ensure that the risk does not pose additional threat to the organization.

TM:SG3.SP2 Address Technology Asset Risks

Risk response plans for risks to technology assets are developed and implemented.

The response to technology asset risk involves the development of strategies that seek to minimize the risk to an acceptable level. This includes reducing the likelihood of risks to technology assets, minimizing exposure to these risks, developing service continuity plans to keep the assets viable during times of disruption, and developing recovery and restoration plans to address the consequences of realized risk.

Because technology assets span a wide range and are pervasive in the organization, risk response strategies may have to be extensive and require significant analysis. For example, addressing the risk that software will fail due to poor design and addressing the physical security of a server require vastly different strategies and implementation considerations.

Risk response for technology assets requires the development of risk strategies and plans (which may include the development of new or revision of existing technology asset controls) and implementing and monitoring these plans for effectiveness.

The subpractices included in this practice are generically addressed in RISK:SG5 in the Risk Management process area.

Typical work products

1. Technology asset risk response plans
2. List of those responsible for addressing and tracking risks

3. Status of technology asset risk response plans

Subpractices

1. Develop and implement risk response plans for all risks that have a "mitigate" disposition.

   Mitigation of operational risks for technology assets will be specific to the technology asset type and where the asset is installed and operating.

   Because there are many categories of technology assets, each of which may have a distinct risk profile, it may be helpful to perform affinity grouping on risks to be addressed before strategies are developed. A simple categorization—segregating by software, hardware, or firmware—can be used, or a more granular convention may be applied.

2. Validate the risk response plans by comparing them to existing strategies for protecting and sustaining technology assets.
3. Identify the person or group responsible for each risk response plan and ensure that they have the authority to act and the proper level of skills and training to implement and monitor the plan.
4. Address residual risk.
5. Implement the risk response plans and provide a method to monitor the effectiveness of these plans.
6. Collect performance measures on the risk management process.

TM:SG4 Manage Technology Asset Integrity

The integrity of technology assets is managed.

The integrity of a technology asset is important to ensuring that the asset is usable for its intended purposes. Whenever technology asset integrity is compromised, the information assets stored, transported, or processed by the asset, as well as the services that depend on the asset, are also potentially compromised. This may be because of loss of functionality, reduced reliability, or impairment of availability when needed.

To be usable for the purposes intended in supporting high-value services, technology assets must possess certain qualities of integrity. They must be

- complete and intact (possessing all of their intended characteristics)
- accurate and valid (being in form and content precisely and exactly as intended)
- authorized and official (approved for use as intended)

The integrity of a technology asset must be considered in the context of the type of asset. Thus, the concept of integrity is applied differently depending on the type of technology asset:

- For software assets, integrity is relative to the modification of the software itself. This includes unauthorized modification of software code, systems, applications, operating systems, tools, and other software-based technology assets.

- For hardware assets, integrity is relative to the modification of either the physical structure of the asset or the configuration parameters of the asset (which are typically considered to be “software” in nature). Modification of the physical structure may occur if cabling is rerouted or a hard drive is replaced. Modification of the configuration parameters may occur if parameters of the operating system are changed to allow use of unauthorized tools or utilities.

Managing technology asset integrity involves controlling access to technology assets, actively managing configuration items, and performing change and release management.

TM:SG4.SP1 Control Access to Technology Assets

Access to technology assets is controlled.

Controlled access to technology assets by authorized staff ensures the continued integrity of these assets by limiting their unauthorized or inadvertent modification.

Access controls for technology assets may take electronic or physical forms. For example, controlling the access to utility programs may prevent changes to a technical asset’s baseline configuration. On the other hand, ensuring that a server is placed behind a physically protected barrier or in a secure room is a physical access control that may prevent destruction of the server or the ability to manipulate configuration settings directly from a console. For software technology assets (and in some cases, firmware), access controls tend to be electronic; for hardware technology assets, access controls can be electronic or physical.

These are examples of actions that require modification access to technology assets:

- modifying or updating software code
- making changes to application system code or modules
- maintaining databases or similar file structures
- modifying the configuration of a server or other hardware
- installing vendor patches to software or firmware
- managing the rulesets of a firewall or similar security device
- modifying the physical configuration of a server or other technical device (such as replacing a hard drive or installing additional memory)
- making modifications to the configuration of physical security systems, including the reprovisioning or deprovisioning of physical access cards and card readers
- making modifications to physical security systems and devices, including cameras and alarm systems

For effectiveness, the organization must thoroughly consider which staff members are authorized to access technology assets and make modifications (based on the unique integrity requirements of each technology asset) and implement electronic and physical controls to meet these requirements. Special consideration must be given to the access needs of information technology staff, who typically have more extensive access to technology assets than they need to perform their job responsibilities. However, because access controls are not infallible, the

organization must also be able to deploy detective controls that allow for logging of modification to technology assets and periodic review of these logs for anomalies.

Managing access is a complementary control to other integrity-focused controls for technology assets such as configuration management, change management, and release management. However, access controls are typically focused on authorizing access to technology assets, while other controls such as configuration management focus on ensuring that modification is systematic, controlled, and monitored.

Typical work products

1. Technology asset access control lists
2. List of staff members authorized to modify technology assets
3. Technology asset modification logs
4. Audit reports

Subpractices

1. Establish access management policies and procedures for requesting and approving access privileges to technology assets.

   The organization should establish policies and procedures for requesting, approving, and providing access to technology assets to 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 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 with a need to know and their responsibilities should be clearly detailed in the policy. The policy should also offer disciplinary measures for violations of the policy.

2. Establish organizationally acceptable tools, techniques, and methods for controlling access to technology assets.

   Selection of the level of configuration control is typically based on objectives, risk, and/or resources. Control levels may vary in relation to the project life cycle, type of system under configuration management, and specific resilience requirements.

3. Identify and document staff who are authorized to modify technology assets relative to the assets' resilience requirements.

   For technology assets, there is additional concern regarding access for information technology or resilience staff. These staff members often are in positions of trust and need to access and make modifications to technology assets (particularly software) to perform their job responsibilities. However, there is often an incorrect assumption that technology and resilience staff need extensive levels of modification privileges, which

can lead to additional risk. These staff members should be specifically identified and their access privileges scrutinized for alignment with their *current* job responsibilities.

4. Perform periodic reviews of technology asset access logs and identify and address anomalies.

TM:SG4.SP2 Perform Configuration Management

The configuration of technology assets is managed.

Configuration management is a fundamental resilience activity. It supports the integrity of technology assets by ensuring that they can be restored to an acceptable form when necessary (perhaps after a disruption) and provides a level of control over changes that can potentially disrupt the assets' support of organizational services. When integrity is suspect for any reason, the resilience of technology assets and associated services may be affected.

Establishing a technology asset baseline (commonly called a "configuration item") provides a foundation for managing the integrity of an asset as it changes over its life cycle. Configuration management also establishes additional controls over the asset so that it is always in a form that is available and authorized for use. In some cases an organization may want to freeze a baseline technology asset configuration, thus permitting no modifications or alterations to the asset over its life cycle.

Configuration management of technology assets is a primary resilience control—it is a means for reconciling the assets' technical and physical attributes with their resilience requirements over time. This may involve all phases of the technology's life cycle, including development phases as well as operations and maintenance, with which configuration control is most often associated. While configuration management for technology assets is focused on the assets themselves (the software, systems, hardware, etc.), it may also naturally extend to other technology work products such as test scripts and plans, asset documentation, and configuration standards and policies.

Configuration management for technology assets is tightly coupled with change control and management. Change control and management is the process of controlling changes to configuration items, which are created and managed in configuration management. Because change control and management is a specialized activity, particularly for technical assets, it is often considered a separate function with its own practices, tools, techniques, and methods. *(Change control for technical assets is addressed in TM:SG4.SP3.)*

The level of control required over technology asset configuration items can range from informal to formal. The level is typically dependent on the type of technology asset, how it is used, where it is deployed, and ultimately the resilience requirements for the asset. Software assets (particularly software code) and application systems tend to require strict levels of configuration control because they are changed frequently and must retain their integrity to be useful for intended purposes. For this reason, configuration

management is a foundational element in software and systems engineering practices.

Configuration management of technology assets involves a range of activities, including

- identifying the configuration of selected assets that compose the baselines at given points in time
- controlling changes to configuration items
- building or providing specifications to the configuration management system
- maintaining the integrity of baseline configurations
- auditing configurations over time to ensure that baselines are updated

Configuration management can be approached at an enterprise level or specifically for each technology asset. The organization must decide the most effective approach and should account for the fact that configuration management for different types of technology assets (i.e., software-based assets versus hardware-based assets) may differ significantly and require separate processes. The content of TM:SG4.SP2 is intended to be applied to all configuration management processes across the range of technology assets that the organization deploys.

Typical work products

1. Standards, policies, and guidelines for technology asset configuration management
2. Identified configuration items
3. Baseline configuration items
4. Configuration control logs and reports
5. Configuration management system, tools, techniques, and methods
6. Configuration audit reports
7. Action items

Subpractices

1. Establish requirements for technology standards, guidelines, and policies for configuration management.

   Selection of the level of configuration control is typically based on objectives, risk, and/or resources. Control levels may vary in relation to the project life cycle, type of system under configuration management, and specific resilience requirements.

   Configuration management should extend to all technology assets, whether developed and implemented in-house or acquired.

2. Establish a configuration management database or system.

   A configuration management system includes the storage media, the procedures, and the tools for accessing the configuration system. The configuration items of the technology assets are stored in the configuration management system (however, this may vary significantly depending on the type of technology asset).

3. Identify the technology assets (configuration items) in detail that will be placed under configuration management.

   A configuration item can be a specific technology asset (such as software code or an operating system) or a series of assets that are related and tied together in a logical baseline configuration item. The organization must plan how it intends to address configuration items for each technical asset type and instantiate guidelines that will ensure consistency of definition and creation of configuration items.

   Configuration items should have specific identifiers and should include important characteristics relevant to the type of technology asset (such as "programming language" for a software code asset).

   These are examples of configuration items that may be placed under configuration control:

   - software and application code
   - application systems (both in operation and in development)
   - operating systems
   - hardware parameters and configuration files
   - firewall rulesets
   - configuration files for routers and other network devices and network routing tables
   - software and hardware tools and utilities
   - policies, manuals, codebooks, and other documents related to technology assets
   - maintenance records for hardware

4. Create baseline configuration items.

5. Track and control changes to configuration items.

   This process includes the establishment of configuration management records and the communication of the contents of these records to appropriate stakeholders.

   This subpractice is typically performed through a formal change control and management process. *(See TM:SG4.SP3.)*

6. Review configuration control logs and identify anomalies.

   Periodically verify (through monitoring and auditing) that changes to configurations are valid and authorized.

7. Perform configuration audits.

   Regularly audit the integrity of the configuration item baselines to ensure that they are complete and correct and that they continue to meet configuration management standards and procedures. Identify action items that are required to repair any anomalies.

TM:SG4.SP3 Perform Change Control and Management

Changes to technology assets are managed.

An important component of configuration management is the ability to control and manage changes to technology assets, particularly to

configuration items. Because of the nature of the operational environment, most technology assets are expected to change over time; the addition of new functionality, the repair of software bugs and security vulnerabilities, or the retirement or replacement of hardware components will alter the original configuration of an asset. Defining and communicating change procedures, including both routine and emergency changes, ensure that changes to technology assets will be handled in an efficient and controlled manner, consistent with organizational policy, standards, and guidelines, with minimum impact on the integrity, availability, and ultimately the resilience of the asset and the services it supports.

Change control and management defines an organizational process that introduces structure and rigor to making changes to technology assets and provides a means for tracking these changes so that problems can be detected and remedied. This provides an enhanced level of confidence in the integrity of the technology assets and their ability to perform their intended functions.

Typical work products

1. Technology asset baseline configuration
2. Change management policies and procedures
3. Change requests
4. Change management database or system
5. Revision history of configuration items
6. Baseline archives

Subpractices

1. Develop and implement change control policies, procedures, and techniques.

   Change requests address not only new or changed requirements but also maintenance and/or failures in the technology assets. Changes are evaluated to ensure that they are consistent with all technical and resilience requirements.

2. Initiate and record change requests in the change control database or system.

   A change management system includes the storage media, the procedures, and the tools for recording and accessing change requests.

3. Analyze the impact of changes proposed in the change requests.

   Change requests are analyzed to determine the impact that the change will have on the resilience requirements, budget, and schedule.

   Changes are also evaluated for their impact beyond immediate project or contract requirements. Changes to a technology used in multiple services can resolve an immediate issue while causing a problem in other applications.

4. Obtain agreement and approval for changes to baselines from relevant stakeholders.

5. Track the status of change requests to closure.

   Ensure that all change requests have a disposition and that changes that have not been closed are provided an updated status.

6. Control configuration items.

   Check in and check out configuration items from the configuration management database or system for incorporation of changes in a manner that maintains the correctness and integrity of the configuration items.

   These are examples of check-in and check-out steps:

   - confirming that the changes are authorized
   - updating the configuration management database
   - archiving the replaced baseline and retrieving the new baseline configuration

   Effective control over configuration items requires proper authentication and access controls to ensure that only those staff members who are authorized are able to check out, make changes to, and check in configuration items. Access management and identity controls must be implemented and managed to ensure that the change process does not cause loss of integrity.

   Access management and identity management are addressed in the Access Management and Identity Management process areas respectively.

   Because the configuration item can be categorized as an information asset, additional controls over information may have to be implemented. *(These controls are addressed in the Knowledge and Information Management process area.)*

TM:SG4.SP4 Perform Release Management

The iteration of technology assets placed into the production environment is managed.

Release management is closely tied to configuration management and change control. While change control addresses the life-cycle process for managing a change request, the result is often a new “release” of a technology asset. Thus, release management addresses the successive release of versions of technology assets into an operations and production environment.

Patch management is a type of release management. Patch management is an important resilience control because it accomplishes two objectives:

1. It ensures that an approved and tested version of a technology asset is placed into production (thereby reducing potential disruptions caused by technology errors).
2. It helps the organization to manage vulnerabilities (particularly in software and systems), which are typically addressed in successive versions of technology assets (thereby reducing exposure to known threats).

Release management requires a process of planning, building, testing, and deploying technology assets and the associated version control and storage of these assets. Release management is intended to be integrated into

configuration management and change control processes so that the organization's ability to control the integrity of technology assets (in order to control operational resilience) is enhanced.

Poor release management can diminish operational resilience by exposing the organization to potential technology asset defects by allowing incorrect or inadequate versions of a technology into production, such as those that are

- older or obsolete
- defective or prone to errors
- subject to known vulnerabilities, threats, and malfunctions
- poorly designed and tested

Typical work products

1. Release management policy, guidelines, and standards
2. Release "builds"
3. Release testing procedures
4. Release build test results

Subpractices

1. Develop and implement guidelines for the appropriate planning and release of technology assets.

   Communicate these guidelines to all staff members who are responsible for the resilience of technology assets.

2. Plan technology asset releases.
3. Develop release builds.

   A release build is the version of the technology asset that is to be released into production. For example, for a software asset, this may be an updated version of an operating system that is being distributed to desktop computers to fix a security flaw. For a hardware asset, a release build may be a newly configured server that is going to be implemented to replace an obsolete server.

   Release builds may be created by the organization or may be acquired from a business partner or vendor.

4. Test release builds.

   To minimize operational impact, the organization must test the release build in a segregated test environment to identify issues, concerns, and problems that may cascade into other operational areas when the build is released. Once all operational issues have been defined and addressed (in some cases by "rebuilding" the build), the organization can proceed to move the release build into the production environment.

5. Move release builds into the organization's production environment.

   This process will differ significantly depending on the type of technology asset that is being released to production.

This process may involve updating configuration item baselines, updating the status of a change request in the change control database or system, and scheduling the physical implementation of the release version into the production environment.

TM:SG5 Manage Technology Asset Availability

The availability of technology assets to support high-value services is managed.

The availability of a technology asset is paramount to supporting organizational services. Information that is stored, transported, or processed by technology assets may be accurate and complete, but if it is not available on demand or in a timely matter, the service may not be able to meet its mission.

There is a distinction between planned downtime and unplanned downtime. Planned downtime is usually the result of a user- or management-initiated event that has been subjected to the change management process. Unplanned downtime typically arises from events or incidents outside the control of the organization such as power outages, security breaches, and disasters like flooding or hurricanes. Unplanned downtime is the effect of diminished operational resilience.

A significantly broad range of operational risks can affect the availability of technology assets for use in supporting high-value services, such as

- accidental or deliberate destruction of the asset
- exposure to natural disaster such as a flood
- operator errors
- software errors, defects, and bugs
- hardware malfunctions or design flaws
- interoperability errors (due to poor integration or interface design)

Many technology assets can be replicated by using spare or easily acquired assets, although cost is a consideration for some assets. Through proper change control and configuration management, organizations may find that the availability of technology assets is controllable, even in light of a range of potential operational risks. However, this is less true of technology assets that are outside of the control of the organization. Resilience requirements must be provided to suppliers to ensure technology asset availability.

To effectively control the operational environment for technology assets, the organization must perform several activities. Foremost, the organization must plan for sustaining technology assets to ensure the continued operation of services. In addition, the organization must address the maintenance of technology assets, the management of technology asset capacity to support current and future service needs, issues related to technology asset complexity and interoperability, and the impact of suppliers and vendors from which technology assets are procured.

TM:SG5.SP1 Perform Planning to Sustain Technology Assets

The availability and functionality of high-value technology assets are ensured through developing plans to sustain them.

Planning for sustaining technology assets can take many forms. The organization may have redundancy for the assets so that when one fails it can easily and quickly substitute another. Or, in the case where this is cost-prohibitive, the organization may have arrangements with outside providers to provide equal or similar services under a shared arrangement. Either way, the organization must ensure that the functionality of technology assets in their support of organizational services can be met as required and specified.

Planning for sustaining technology assets can be integrated into the development of service continuity plans for services or instantiated in plans specifically focused on high-value technologies. How this planning is performed may depend on the organization's overall approach to service continuity planning, the types of technology assets the plan addresses, the services that the technology assets support, and the level of planning being performed (i.e., enterprise, organizational unit, IT, etc.). For example, the organization may choose to develop service continuity plans for application systems as a part of developing plans for high-value services that rely on these applications. However, this becomes more difficult if more than one service relies on a single application; when this situation of shared technology assets results, the organization may streamline its approach and develop continuity plans for the shared assets upon which related services can then develop their own specific but referenced plans.

With respect to technology assets, there is a wide range of service continuity plans that may have to be developed. These plans may be developed specifically by asset type, or they can be bundled with the development of service continuity plans for services. In some cases, because a technology asset is shared (such as a network), the organization may have a specific plan that covers the enterprise asset for all services. These are examples of the technology assets that may be addressed specifically:

- desktop computers and related hardware
- organizational application systems (related software code and specialized equipment)
- productivity software such as email systems and word processing systems
- networks (servers, routers, cabling, and other related equipment)
- telecommunications equipment and software (including telecommunications infrastructure, phone systems, satellite communications, and cellular communications)
- processing hardware, including mainframes, servers, and their related assets such as operating systems
- disk drives and storage hardware and software
- printers and fax machines (particularly those that are high-value)
- security-specific systems, applications, utilities, and tools
- specialized equipment such as card readers, cash registers and point-of-sale terminals, and other technology that supports services

The development and management of service continuity plans are addressed in the Service Continuity process area. This practice may not be able to be completed unless consideration of the practices in the Service Continuity process area has been made.

Typical work products

1. Results of business impact analysis or risk assessment
2. Availability metrics for technology and related services
3. Recovery time objectives (RTOs)
4. Recovery point objectives (RPOs)
5. Service continuity plans (specifically addressing activities to sustain technology assets)

Subpractices

1. Develop an approach for sustaining technology assets.

   Technology assets are pervasive and tend to be linked to services; thus, the organization must determine how it will approach planning to sustain these to ensure that all high-value assets are addressed. This may involve separating technology assets into those that are shared and those that are proprietary (i.e., to a specific organizational unit or to support a specific service). Performing business impact analysis at the organizational unit level may give the organization some understanding of shared versus proprietary technology assets, and this information can be used in determining the best approach.

2. Establish availability metrics for high-value technology assets.

   Availability metrics establish the planned and required "uptime" for a technology asset. They are typically established as part of the asset's resilience requirement for availability and may be developed with consideration of the services that the asset supports.

   While availability metrics are most useful for managing technology assets in operation, they also play a significant part in the development of plans to sustain technology assets in that they establish a parameter or target that must be attained by technology assets under disruptive conditions. In other words, the availability metric must be met by an asset not only in day-to-day operations but sometimes also under diminished conditions brought on by a disruption or event. These metrics must be considered in planning to determine whether they can be met under diminished conditions and, if not, what additional steps the organization may need to take (e.g., implement manual procedures) to ensure that associated services are not affected.

   Resilience requirements that would include the availability requirement for technology assets are developed and managed respectively in the Resilience Requirements Development and the Resilience Requirements Management process areas.

3. Establish recovery time objectives for high-value technology assets.

   Recovery time objectives (RTOs) establish the period of acceptable downtime of a technology asset (and typically the associated service), after which the organization will suffer an unwanted consequence or impact. RTOs are typically developed at the service level but will be inherited by technology assets that support these services.

RTOs must be included in service continuity plans to establish the tolerances within which the plan must be operable.

4. Establish recovery point objectives for high-value technology assets.

   Recovery point objectives (RPOs) establish the point to which a technology asset must be restored to allow recovery of the asset and associated services after a disruption. RPOs must be developed and considered in service continuity plans, particularly restoration plans.

5. Develop service continuity plans that address technology availability.

   Depending on the organization's focus, service continuity plans can be specifically developed for high-value technology (which would affect associated services) or may be developed from a services viewpoint (which addresses technology as an associated asset).

TM:SG5.SP2 Manage Technology Asset Maintenance

Operational maintenance is performed on technology assets.

Meeting the availability requirements of technology assets (particularly hardware) typically requires the performance of regular maintenance activities. While these activities are typically physical in nature (for example, cleaning disk drives to ensure they do not have a mechanical failure), some maintenance may be virtual or electronic, such as when software patches are applied to optimize code performance. *(See patch management in TM:SG4.SP4.)* The criteria used to establish guidelines for maintenance are performed relative to the value of the related services supported by the assets that are located in the facility.

Several types of maintenance may be required based on the type of technology asset. These types of maintenance include

- corrective maintenance (i.e., correcting and repairing problems that degrade the operational capability of the technology)
- preventive maintenance (i.e., preventing potential technology problems from occurring through preplanned activities)
- adaptive maintenance (i.e., adapting technology assets to a different operating environment)
- perfective maintenance (i.e., developing or acquiring an additional or improved operational capability from the technology)

While regular maintenance on technology assets is an important component of ensuring availability, these activities also often bring additional risk because of errors, inadvertent actions, or deliberate actions. All maintenance activities to technology assets should be controlled, monitored, and authorized.

Technology assets included in facilities may be included as part of a facility's regular maintenance schedule and process. Thus, in some organizations, facility maintenance may encompass technology asset maintenance, particularly in facilities such as data centers where technology is integral to the facility. In this case, the organization's facility

and technology asset maintenance programs should be coordinated. *(Maintenance to facility assets is addressed in the Environmental Control process area.)*

Typical work products

1. List of technology assets requiring regular maintenance
2. Equipment service intervals and specifications
3. List of maintenance staff authorized to carry out repairs and service
4. Documented maintenance records
5. Maintenance change requests

Subpractices

1. Identify technology systems that require regular maintenance activities.
2. Document equipment suppliers' recommended service intervals and specifications.
3. Document a list of maintenance staff authorized to carry out repairs and service.

   Maintenance staff should be subject to the organization's standards for authorizing and providing access. *(The management of access controls is addressed in the Access Management process area.)*

4. Document all suspected or actual faults and all preventive, corrective, and other types of maintenance.

   Maintenance records should be retained for all technology assets and stored appropriately with access only to authorized individuals. Risks related to software systems and their maintenance may need additional analysis and resolution.

   These activities may result in additions or revisions to existing service continuity plans or may require separate plans to be developed. Actions that are required for service continuity planning should be identified and executed as part of this activity.

5. Implement maintenance and test maintenance changes in a non-operational environment when appropriate.
6. Establish appropriate controls over sensitive or confidential information when maintenance is performed.

   Maintenance activities can result in often-undetected vulnerabilities to information assets. All controls over information assets should be reaffirmed before maintenance is performed, and information access and modification logs should be checked after maintenance is performed.

   Appropriate controls over information assets are addressed in the Knowledge and Information Management process area.

7. Communicate maintenance changes to appropriate entities.
8. Implement maintenance according to change request procedures.
9. Document and communicate results of maintenance.

TM:SG5.SP3 Manage Technology Capacity

The operating capacity of technology assets is managed.

Capacity is a significant factor in meeting the availability requirements of technology assets and in turn of the services that rely on these assets. The operating capacity of technology assets must be managed commensurate with operational demands to support services; otherwise these services will be affected by diminished operability and potentially fail to meet their missions.

Capacity planning and management involve measuring current demand, testing for anticipated demand, and gathering usage trends over time to be able to predict expansion needs. Consideration of capacity to ensure technology availability and meet business objectives requires a proactive approach to managing demand and anticipating future needs.

Capacity planning often takes into account that demand is widely variable and that technology assets may need to meet a wide range of capacity needs in operation. This variation is typically due to changing organizational and operational conditions, many of which are out of the direct control of the organization. For example, the following are common organizational events that could affect the capacity of technology assets:

- staff changes that require changes to technology assets, such as the addition of new users (either internally or externally), the transfer of existing staff members from one organizational unit to another, or the termination of staff members
- changes to information such as the creation, alteration, or deletion of paper and electronic records, files, and databases that are stored, transported, or processed by technology
- new service demands, such as launching a new product line or service, that tax the transaction processing capability of systems and networks
- technology refresh, such as the addition of new technical components (particularly new application systems) or changes to existing technical components
- technology retirement
- security events, such as a denial-of-service attack, that could diminish operating capacity

Capacity planning and management require a strategic view to ensure consideration of the organization's strategic objectives and their impact on technology is addressed. A strategy for capacity management also requires the selection of measures and analytic techniques to support availability and capacity management objectives and the establishment and maintenance of technology asset baselines and models to understand current capacity, availability, and levels of service provision (i.e., describe what the normal capacity, availability, and service levels are). In addition to understanding the capacity and availability of the technology assets, forecasting is done for future capacity, availability, and service levels based on trends in service resource use, service system performance, and business process requirements.

Typical work products

1. Capacity management strategy
2. Capacity forecasts
3. Capacity statistics and performance metrics

Subpractices

1. Identify technology assets that require capacity management and planning.
2. Document technology asset use, performance, capacity, and availability needs.

   This practice may result in updated performance and availability metrics and changes to RTOs and RPOs for related services.

3. Forecast technology asset use, performance, capacity, and availability needs.
4. Develop a strategy to meet the demand for capacity based on the resilience requirements for the technology asset and the services it supports.

   In this case, the strategy may need to consider the organization's strategic objectives and how the accomplishment of these objectives affects capacity of current technology assets and future capacity needs.

5. Periodically validate and update the capacity management strategy for technology assets based on operational and organizational environment changes.

TM:SG5.SP4 Manage Technology Interoperability

The interoperability of technology assets is managed.

Technology assets rarely operate in isolation in organizations; instead, they are typically dependent on the services of other technology assets to support an organizational service. As a simple example, consider a server that supports a web service—it must be connected to a network and user interfaces such as personal computers to provide the service. Thus, these technology assets must be connected and interoperable to meet a shared goal.

In reality, most organizations have significant levels of technology complexity and interconnection where virtually all technology assets have some connection between them, particularly with assets such as application systems. Concepts such as "systems of systems" acknowledge the need for formal coordination of technology components toward a desired organizational outcome. This required interoperability creates another fundamental challenge for the organization in managing operational resilience.

The failure to actively identify and address issues related to interoperability poses an additional level of operational risk to the organization that can result in disruption of organizational services. Unfortunately, issues related

to interoperability are often unknown until an unwanted outcome (such as when software code fails or produces an unexpected result) is realized by the organization. Thus, the organization must seek to actively identify interoperability issues and proactively address them before they cause degraded performance or service failures.

Managing interoperability of technology assets requires the organization to develop and maintain a strategy for identifying, analyzing, and addressing operational risks related to technology asset interoperability. Some of the actions the organization must take are development-related—accurately defining interfaces, providing standards for design and architecture, and performing extensive testing. Other actions are review-focused in that the organization must actively seek to identify interoperability issues that have not yet been uncovered or realized so that they can be neutralized before they pose danger, including issues related to single points of failure and operational bottlenecks.

Typical work products

1. Architecture interoperability standards
2. Enterprise architecture steering committee
3. Interoperability risk management strategy

Subpractices

1. Establish interoperability standards.

   Interoperability standards provide the organization a means to enforce architecture and design principles that seek to minimize the effects of complexity and technology interoperability. These standards seek to prevent operational risks that result from interoperability as well as to provide the organization a level of control over permissible connections and complexity in accordance with the organization's risk tolerance. Standards may address issues such as

   - design, development, and implementation of interoperability-friendly architectures
   - appropriate integration of systems (either designed in-house or acquired)
   - appropriate interface design
   - requirements for data sharing and integrity across technology platforms and architectures
   - means for analyzing connections and identifying problems
   - guidelines for establishing and managing systems of systems
   - methods for identifying and analyzing risks

2. Develop interoperability management strategy.

   The interoperability strategy determines how the organization is going to address issues of interoperability and the standards and guidelines for interoperability that will be used across the enterprise. The strategy should include provisions for regular assessment of technology platform architectures to determine potential failure points and should establish an enterprise architecture steering committee or similar construct to ensure that there is specific governance over interoperability issues.

3. Identify and analyze risks related to interoperability of technology assets.

   The identification of risks that emanate from interoperability issues and concerns should be integrated into the organization's enterprise operational risk management strategy. The identification and analysis of these risks should be focused on

   - identifying behavioral patterns such as
     - unexpected or incorrect process outputs
     - significant processing failures or performance issues
     - increased levels of "unplanned" system or asset downtime
   - identifying and analyzing single points of failure caused by incompatible processes or "handshakes"
   - identifying processing or communications bottlenecks resulting from interoperability "choke" points

   Risks identified as related to interoperability issues should be managed through the organization's regular risk management process as defined in the Risk Management process area.

4. Monitor the interoperability strategy on a regular basis to ensure that it does not pose additional risks to the organization.

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 Technology Management process area.

TM:GG1 Achieve Specific Goals

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

TM:GG1.GP1 Perform Specific Practices

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

Elaboration:

Specific practices TM:SG1.SP1 through TM:SG5.SP4 are performed to achieve the goals of the technology management process.

TM:GG2 Institutionalize a Managed Process

Technology management is institutionalized as a managed process.

TM:GG2.GP1 Establish Process Governance

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

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

Subpractices

1. Establish governance over process activities.

   Elaboration:

   Governance over the technology management process may be exhibited by

   - establishing a higher level position, often the chief information officer, responsible for the resilience of the organization's technology assets
   - developing and publicizing higher level managers' objectives and requirements for the process
   - oversight over the development, acquisition, implementation, and management of high-value technology assets
   - sponsoring and providing oversight of policy, procedures, standards, and guidelines for the documentation of technology assets and for establishing asset ownership and custodianship
   - 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
   - oversight over the establishment, implementation, and maintenance of the organization's internal control system for technology assets
   - sponsoring and funding process activities
   - implementing a technology steering committee
   - providing guidance for prioritizing technology assets relative to the organization's high-priority strategic objectives
   - providing guidance on identifying, assessing, and managing operational risks related to technology assets
   - providing guidance for resolving violations of technology asset integrity and availability requirements
   - 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
   - conducting regular internal and external audits and related reporting to appropriate committees on technology asset controls and the effectiveness of the process

- 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 technology management policy should address

- responsibility, authority, and ownership for performing process activities
- procedures, standards, and guidelines for
  - documenting and maintaining technology asset descriptions and relevant information
  - describing and identifying technology owners and custodians
  - developing and documenting resilience requirements for technology assets
  - establishing, implementing, and maintaining an internal control system for all technologies, including configuration, change, and release management
  - maintaining environmental conditions for physical technologies (hardware, infrastructure)
  - managing technology asset operational risk
  - establishing technology asset service continuity plans and procedures
  - retiring technology assets at the end of their useful life
  - architectural interoperability
  - removing technology assets from the workplace
- the association of technology assets to core organizational services, and the prioritization of assets for service continuity
- requesting, approving, and providing access to technology assets to persons, objects, and entities, including type and extent of access and requests that originate externally to the organization *(Refer to the Access Management process area for more information about granting access [rights and privileges] to technology assets. Refer to the Identity Management process area for more information about creating and maintaining identities for persons, objects, and entities.)*
- methods for measuring adherence to policy, exceptions granted, and policy violations

TM:GG2.GP2 Plan the Process

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

Elaboration:

A plan for performing the technology management process is created to preserve the integrity of technology assets and to ensure that technology assets remain available and viable to support organizational services. The plan must address the resilience requirements of the technology assets, dependencies of services on these assets, and consideration of multiple asset owners and custodians at various levels of the organization. In addition, because technology assets may have a strong geographical

connection, the plan must extend to external stakeholders that can enable or adversely affect technology resilience.

The plan for the technology management process should not be confused with service continuity plans for classes of or specific technology assets. The plan for the technology management process details how the organization will perform technology management, including the development of service continuity plans for technology assets. *(The generic practices for service continuity planning are described in SC:SG1 through SC:SG4 in the Service Continuity process area.)*

Subpractices

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

   Elaboration:

   Special consideration in the plan may have to be given to establishing, implementing, and maintaining an internal control system for technology assets and for sustaining technology assets. These activities address actions required to protect and sustain technology assets commensurate with their resilience requirements.

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

TM:GG2.GP3 Provide Resources

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

Elaboration:

The diversity of activities required to protect and sustain technology assets requires an extensive level of organizational resources and skills and a significant number of external resources. In addition, these activities require a major commitment of financial resources (both expense and capital) from the organization.

Subpractices

1. Staff the process.

   Elaboration:

   These are examples of staff required to protect and sustain technology assets:

   - staff responsible for
     - information, application, hardware, and technical security
     - business continuity and disaster recovery
     - IT operations and service delivery
     - implementing and maintaining technology asset security controls (such as security-trained network and system administrators)
     - configuration management, change management, and release management of technology assets
     - establishing and maintaining physical security (such as security guards)

  - implementing and maintaining physical security access and surveillance systems
- staff involved in technology risk management, including insurance and risk indemnification staff
- facilities management staff for physical technology assets (hardware, infrastructure)
- contractors responsible for developing, implementing, and maintaining technology assets
- owners and custodians of technology assets (to identify and enforce resilience requirements)

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.

Elaboration:

At a minimum, funding must be available to support the development, implementation, testing, and execution of service continuity plans for technology assets. In some cases, capital funding may be required for projects that enhance or support actions to protect and sustain technology assets, which may result in developing additional facilities (to protect tangible technical assets) or establishing outsourcing contracts to support facilities when needed.

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

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

Elaboration:

Keep in mind that tools used to support the technology management process are themselves technology assets that have to be managed according to the process.

These are examples of tools, techniques, and methods so support the technology management process:

- methods and techniques for prioritizing technology assets
- methods, techniques, and tools for managing risks to technology assets, including tracking open risks to closure and monitoring the effectiveness of technology asset risk response plans
- methods, techniques, and tools for creating and maintaining the technology asset inventory, including database systems
- methods, techniques, and tools for maintaining technology assets, including asset configuration management, change control, release management, and monitoring and logging of modification activities
- methods, techniques, and tools for controlling access to technology assets
- methods for establishing, implementing, and maintaining the internal control system for technology assets

- methods for the proper retirement and disposal of technology assets
- methods, techniques, and tools for technology asset backup, retention, and restoration
- methods, techniques, and tools for managing technology assets that are provided by external entities

TM:GG2.GP4 Assign Responsibility

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

Elaboration:

Of paramount importance in assigning responsibility for the technology management process is the establishment of technology asset owners and custodians *(which is described in ADM:SG1.SP3)*. Owners are responsible for establishing technology asset resilience requirements, ensuring these requirements are met by custodians, and identifying and remediating gaps where requirements are not being met. Owners may also be responsible for establishing, implementing, and maintaining an internal control system commensurate with meeting technology asset resilience requirements if this activity is not performed by a custodian.

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.

Refer to the Asset Definition and Management process area for more information about establishing ownership and custodianship of technology assets.

Subpractices

1. Assign responsibility and authority for performing the process.

   Elaboration:

   Responsibility and authority may extend not only to staff inside the organization but to those with whom the organization has a contractual (custodial) agreement for developing, implementing, and managing technology assets (including implementation and management of controls, including those to sustain technology assets).

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

   Elaboration:

   Responsibility and authority for performing technology 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 organizational unit managers, line of business managers, project managers, and asset and service owners and custodians to participate in the process for assets under their ownership or custodianship

- developing and implementing contractual instruments (as well as service level agreements) with external entities to establish responsibility and authority for outsourced technology assets
- including process tasks in staff performance management goals and objectives, with requisite measurement of progress against these goals
- developing and implementing contractual instruments (as well as service level agreements) with external entities to establish responsibility and authority for technology assets, where applicable
- including process tasks in measuring performance of external entities against service level agreements *(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.

TM:GG2.GP5 Train People

Train the people performing or supporting the technology 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:

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

   - prioritization and categorization of technology assets
   - knowledge of tools, techniques, and methods that can be used to identify, analyze, address, and monitor operational risks to technology assets
   - establishing, implementing, and maintaining the internal control system for technology assets
   - protecting and sustaining technology assets to meet their integrity and availability requirements
   - operating and maintaining all categories of technology assets (hardware, software, systems, infrastructure, and tools)

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:

   - technology asset risk management concepts and activities (e.g., risk identification, analysis, response, and monitoring)

- technology asset definition, prioritization, and handling
- technology asset resilience requirements development
- establishing, implementing, and maintaining internal controls for protecting and sustaining technology assets
- cross-training to ensure adequate knowledge and coverage for all technology assets and their operation
- proper techniques for technology asset disposal
- technology asset configuration, change, and release management
- supporting technology asset owners and custodians in understanding the process and their roles and responsibilities with respect to its activities
- working with external entities that have responsibility for process activities
- using process methods, tools, and techniques, including those identified in TM:GG2:GP3 subpractice 3

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

TM:GG2.GP6 Control Work Products

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

Elaboration:

All work products related to technology asset administrative, technical, and physical controls (configurations, change requests, logs, policies, standards, etc.) should be placed under control.

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

- inventory of high-value and resilience technology assets
- integrity and availability requirements
- administrative, technical, and physical controls
- list of operational risks by asset and asset category with prioritization, risk disposition, response plans, and current status
- risk statements with impact valuation
- access control lists
- modification logs and audit reports
- baseline configuration items and configuration control logs and reports
- configuration management, change management, and release management systems
- baseline archives and backup media
- release builds, testing procedures, and release build test results
- recovery time and recovery point objectives
- service continuity plans
- equipment service intervals and specifications
- capacity forecasts, statistics, and performance metrics
- process plan
- policies and procedures
- contracts with external entities

Refer to the Environmental Control process area for more information about managing physical technology assets (such as hardware and infrastructure) that reside in facilities.

TM:GG2.GP7 Identify and Involve Relevant Stakeholders

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

Subpractices

1. Identify process stakeholders and their appropriate involvement.

   Elaboration:

   Because technology assets may reside in a wide range of physical locations and be developed and maintained by internal and external entities, a substantial number of stakeholders are likely to be external to the organization.

   These are examples of stakeholders of the technology management process:

   - owners and custodians of technology assets
   - service owners
   - organizational unit and line of business managers responsible for high-value technology assets and the services they support
   - staff responsible for managing operational risks to technology assets
   - staff responsible for establishing, implementing, and maintaining an internal control system for technology assets, including those responsible for configuration, change, and release management
   - staff required to develop, test, implement, and execute service continuity plans for technology assets
   - external entities such as public service providers, public infrastructure providers, and contractors that provide essential facility services such as those related to maintaining environmental conditions for physical technology assets (hardware, infrastructure)
   - staff in other organizational support functions, such as accounting or general services administration (particularly as related to technology inventory valuation and retirement)
   - internal and external auditors

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

   - planning for the process
   - creating a technology asset baseline
   - creating technology asset profiles and asset risk and vulnerability profiles
   - associating technology assets with services and analyzing service dependencies
   - assigning resilience requirements for technology assets
   - establishing, implementing, and managing technology asset controls
   - developing service continuity plans for technology assets
   - managing operational risks to technology assets
   - managing technology asset configurations, changes, and releases

- controlling the operational environment in which technology assets reside
- managing technology asset external dependencies for assets developed, operated, and maintained by external entities
- managing relationships with external entities that provide technology asset services
- reviewing and appraising the effectiveness of process activities
- resolving issues in the process

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

TM:GG2.GP8 Measure and Control the Process

Measure and control the technology 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 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 technology management process:
   - percentage of technology assets that have been inventoried
   - percentage of technology assets with/without a complete asset profile (such as no stated resilience requirements)
   - percentage of technology assets with/without a designated owner
   - percentage of technology assets with/without a designated custodian
   - percentage of technology assets that have designated owners but no custodians
   - percentage of technology assets that have designated custodians but no owners
   - percentage of technology assets that have been inventoried, by service
   - percentage of technology assets that are not associated with one or more services
   - percentage of technology asset-service dependency conflicts with unimplemented or incomplete mitigation plans
   - number of discrepancies between the current inventory and the previous inventory
   - number of changes made to asset profiles in the technology asset inventory

- number of changes to resilience requirements as a result of technology asset changes
- number of changes to service continuity plans as a result of technology asset changes
- percentage of technology assets that are designated as high-value assets
- elapsed time since the technology asset inventory was last reviewed
- elapsed time since review and validation of high-value technology assets and their priorities
- elapsed time since review and reconciliation of resilience-focused technology assets (those required for service continuity & service restoration)
- percentage of technology assets without assigned/defined resilience requirements
- percentage of technology assets with assigned/defined resilience requirements that are undocumented
- percentage of technology assets that do not satisfy their resilience requirements
- percentage of technology assets with no or missing protection controls
- percentage of technology assets with no or missing sustainment controls
- percentage of technology asset controls (protection and sustainment) that are ineffective or inadequate as demonstrated by:
  - unsatisfied control objectives
  - unmet resilience requirements
  - outstanding control assessment problems areas above established thresholds and without remediation plans
- percentage of technology asset control deficiencies not resolved by scheduled due date (refer to CTRL measures for categories of control deficiencies)
- elapsed time since review of the effectiveness of technology asset controls
- elapsed time since risk assessment of technology assets performed
- elapsed time since business impact analysis of technology assets performed
- percentage of technology assets for which business impact valuation (qualitative or quantitative) has not been performed
- percentage of technology assets for which a risk assessment has not been performed and documented (per policy or other guideline) and according to plan
- percentage of technology asset risks that have not been assigned to a responsible party for action, tracking, and closure
- percentage of technology asset risks with a disposition of “mitigate” that do not have a defined response plan
- percentage of technology asset risks with a “mitigate” disposition that are not effectively addressed by their response plans
- percentage of realized risks for technology assets that exceed established risk parameters
- number of violations of access control policies for technology assets
- percentage of intrusions into digital technology assets where impact exceeds threshold
- percentage of intrusions into physical technology assets where impact exceeds threshold
- elapsed time since audit of technology asset modification logs
- percentage of technology assets for which approved configuration settings have/have not been implemented as required by policy

- percentage of technology assets with configurations that deviate from approved standards for which exceptions have not been granted
- elapsed time since review of technology asset configuration control logs
- elapsed time since audit of technology asset configurations
- number of unauthorized changes to technology assets (may need to report by some meaningful categorization of assets)
- change success rate (percentage of changes to technology assets that succeed without causing an incident, service outage, or impairment)
- percentage of changes that are high-priority, emergency changes
- percentage of changes that result from deficiencies in resilience requirements
- elapsed time between:
  - scheduled technology asset configuration updates and actual configuration updates
  - scheduled technology asset changes and actual changes
  - scheduled technology asset releases into production and actual releases

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

   Elaboration:

   Reviews will likely verify the accuracy and completeness of the technology asset inventory.

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

   - newly acquired technology assets are included in the inventory
   - changes to technology assets (additions, modifications, and retirements) are accurately reflected in the inventory
   - technology assets have stated resilience requirements
   - asset-service mapping is accurate and current
   - ownership and custodianship over technology assets are established and documented
   - administrative, technical, and physical controls are operating as intended
   - controls are meeting the stated intent of the resilience requirements
   - status reports are provided to appropriate stakeholders in a timely manner
   - technology asset issues 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
   - 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.
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.

   Elaboration:

   For technology assets, corrective action may require the revision of existing administrative, technical, and physical controls, development and implementation of new controls, or a change in the type of controls (preventive, detective, corrective, compensating, etc.).

7. Track corrective action to closure.

TM:GG2.GP9 Objectively Evaluate Adherence

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

Elaboration:

These are examples of activities to be reviewed:

- identifying and prioritizing technology assets
- identifying technology requirements
- establishing and implementing technology asset controls
- identifying and managing technology asset risks
- developing service continuity plans for technology assets
- identifying and managing technology asset dependencies
- identifying and managing changes to technology assets
- retiring technology assets
- aligning stakeholder requirements with technology management process plans
- assigning responsibility, accountability, and authority for technology management process activities
- determining the adequacy of technology management reports and reviews in informing decision makers regarding the performance of operational resilience management activities and the need to take corrective action, if any
- verifying technology management controls
- using technology management work products for improving technology asset protection and sustainment strategies

These are examples of work products to be reviewed:

- technology asset inventory
- technology asset internal controls documentation
- technology asset risk statements
- technology asset risk response plans
- service continuity plans for technology assets
- technology asset maintenance records and change logs
- business impact analysis results for technology assets
- lists of key providers and contacts for technology assets
- technology asset retirement standards

- contracts with external entities
- technology management process plan and policies
- technology asset issues that have been referred to the risk management process
- technology management methods, techniques, and tools
- metrics for the technology management process *(Refer to TM:GG2.GP8 subpractice 2.)*

TM:GG2.GP10 Review Status with Higher Level Managers

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

Elaboration:

Status reporting on the technology management process may be part of the formal governance structure or may be performed through other organizational reporting requirements (such as through the chief risk officer or the chief resilience officer level). Audits of the process—particularly the validation of the organization's technology asset inventory and internal control system at points in time—may be escalated to higher level managers through the organization's audit committee of the board of directors or similar construct in private or non-profit organizations.

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

TM:GG3 Institutionalize a Defined Process

Technology management is institutionalized as a defined process.

TM:GG3.GP1 Establish a Defined Process

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

Elaboration:

Technology management is typically carried out at the organizational unit or line of business level for convenience and accuracy and may have to be geographically focused (because of the location of specific technology assets). However, to achieve consistent results in creating and managing technology assets, the activities at the organizational unit or line of business level must be derived from an enterprise definition of the technology management process. The technology asset inventory may be inconsistent across organizational units, particularly when assets have shared ownership across organizational lines, but the defined process remains consistent. The level of completeness and accuracy of technology asset descriptions across organizational units may affect asset management at the enterprise level and impede operational resilience.

In addition, a variable mix of administrative, technical, and physical controls may be used across the organization to meet the resilience requirements for technology assets, but the process is consistent with the enterprise definition.

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 technology 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.

TM:GG3.GP2 Collect Improvement Information

Collect technology 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:

- technology asset inventories
- inventory inconsistencies and issues
- reports on the effectiveness and weaknesses of controls
- improvements based on risk identification and mitigation
- effectiveness of technology asset service continuity plans in execution
- metrics and measurements of the viability of the technology management process *(Refer to TM:GG2.GP8 subpractice 2.)*
- changes and trends in operating conditions, risk conditions, and the risk environment that affect technology management results
- lessons learned in post-event review of technology asset incidents and disruptions in continuity
- maintenance issues and concerns for technology assets
- conflicts and risks arising from dependencies on external entities
- lessons learned in updating, replacing, and retiring technology assets from active use
- resilience requirements that are not being satisfied for technology assets 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.