Software Engineering Institute

CERT® Resilience Management Model, Version 1.2

Knowledge and Information Management (KIM)

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/

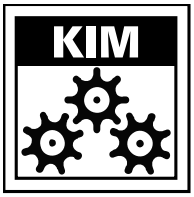
Carnegie Mellon

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

KNOWLEDGE AND INFORMATION MANAGEMENT

Operations



Purpose

The purpose of Knowledge and Information Management is to establish and manage an appropriate level of controls to support the confidentiality, integrity, and availability of the organization's information, vital records, and intellectual property.

Introductory Notes

The importance of information as an organizational asset continues to grow. The focus of organizations has increasingly turned to intangible assets such that the ratio of tangible assets to intangible assets continues to decrease. This supports the assertion that information is one of the most—if not the most—high-value organizational assets. It is the raw material that is used by and created in services. The protection of this intellectual and enterprise capital—to ensure that it is available in the form intended for use in services—is the focus of the Knowledge and Information Management process area.

An information asset can be described as information or data that is of value to the organization, including such diverse information as patient records, intellectual property, vital business records and contracts, and customer information. The unique aspect of information assets is that they can exist in physical form (on paper, CDs, or other media) or electronic form (files, databases, on personal computers). The Knowledge and Information Management process area addresses the importance of information assets in the operational resilience of services, as well as unique attributes specific to information assets such as those described in Table KIM-1.

Table KIM-1 Attributes of Information Assets

Attribute	Description
Confidentiality	For an information asset, the quality of being accessible only to authorized people, processes, and devices
Integrity	For an information asset, the quality of being in the condition intended by the owner and so continuing to be useful for the purposes intended by the owner
Availability	For an information asset, the quality of being accessible to authorized users (people, processes, or devices) whenever it is needed
Privacy	The assurance that information about an individual is disclosed only to people, processes, and devices authorized by that individual or permitted under privacy laws and regulations
Sensitivity	A measure of the degree to which an information asset must be protected based on the consequences of its unauthorized access, modification, or disclosure

In this process area, information assets are prioritized according to their value in supporting high-value organizational services. Physical, technical, and administrative controls that keep information assets viable and sustainable are selected, implemented, and managed, and the effectiveness of these controls is monitored. In addition, information asset risks are identified and addressed in an attempt to prevent disruption when possible. Information is categorized as to its organizational sensitivity, and consideration is given to the backup and storage of

important information and vital records in case of loss or destruction, or to support the execution of service continuity plans.

Knowledge management is also performed in this process area: the requirement to identify and document the organizational and intellectual knowledge of staff that is important to the effective operation of the organization's services. This information asset is often not documented, has poorly developed security requirements, and lacks adequate protection. It is also often one of the most high-value information assets in the organization.

Related Process Areas

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

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

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

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

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

Summary of Specific Goals and Practices

Goals	Practices
KIM:SG1 Establish and Prioritize Information Assets	KIM:SG1.SP1 Prioritize Information Assets
	KIM:SG1.SP2 Categorize Information Assets
KIM:SG2 Protect Information Assets	KIM:SG2.SP1 Assign Resilience Requirements to Information Assets
	KIM:SG2.SP2 Establish and Implement Controls
KIM:SG3 Manage Information Asset Risks	KIM:SG3.SP1 Identify and Assess Information Asset Risks
	KIM:SG3.SP2 Address Information Asset Risks
KIM:SG4 Manage Information Asset Confidentiality and Privacy	KIM:SG4.SP1 Encrypt High-Value Information
	KIM:SG4.SP2 Control Access to Information Assets
	KIM:SG4.SP3 Control Information Asset Disposition
KIM:SG5 Manage Information Asset Integrity	KIM:SG5.SP1 Control Modification of Information Assets
	KIM:SG5.SP2 Manage Information Asset Configuration
	KIM:SG5.SP3 Verify Validity of Information
KIM:SG6 Manage Information Asset Availability	KIM:SG6.SP1 Perform Information Duplication and Retention
	KIM:SG6.SP2 Manage Organizational Knowledge

Specific Practices by Goal

KIM:SG1 Establish and Prioritize Information Assets

Information assets are prioritized to ensure the resilience of high-value services in which they are used.

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

Prioritization of information assets is a risk management activity. It establishes the information assets that are of most value to the organization and for which measures to protect and sustain them are required. Failure to prioritize information assets may lead to inadequate operational resilience of high-value assets and excessive levels of operational resilience for non-high-value assets.

Information assets may also be of high priority to the organization because of their sensitivity. The unique nature of these information assets may require a higher level of resilience controls.

KIM:SG1.SP1 Prioritize Information Assets

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

The prioritization of information 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 disruption has the potential to cause the most significant organizational consequences.

Information asset prioritization is performed relative to services—that is, information assets associated with high-value services are those that must be most highly prioritized for operational resilience activities.

However, the organization can use other criteria to establish high-priority information assets, such as

- the use of the asset in the general management and control of the organization (contracts, articles of incorporation, etc.)
- highly sensitive or classified information *(Categorization of information assets is addressed in KIM:SG1.SP2.)*
- information that represents the organization's trade secrets or proprietary information such as intellectual property *(Intellectual property management is addressed in KIM:SG4.SP2.)*
- information assets that are of high value to more than one service
- value of the asset in directly supporting the organization's achievement of critical success factors and strategic objectives
- the organization's tolerance for "pain"—the degree to which it can suffer a loss or destruction of the information asset and continue to meet its mission

Typically, the organization selects a subset of information assets from its asset inventory; however, the organization could compile a list of high-value information 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 information assets may never have been inventoried. *(The identification, definition, management, and control of information assets are addressed in the Asset Definition and Management process area.)*

Typical work products

1. List of high-value information assets

Subpractices

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

   These assets should include those that would be required for the successful execution of service continuity plans. Assets that are generally important to the successful operation of the organization (vital records, contracts, etc.) should also be included in the organization's list. The list of high-value information assets should be the focus of operational risk and resilience activities.

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

KIM:SG1.SP2 Categorize Information Assets

Information assets that support high-value services are categorized as to their organizational sensitivity.

The categorization of information assets is a key consideration in the development of adequate resilience requirements and in the implementation of strategies to protect and sustain them.

An information sensitivity categorization scheme and the corresponding information handling processes and procedures provide a way for the organization to put its mark on information assets relative to their risk tolerances and to allow for an appropriate level of corresponding handling, protection, and resilience. Failure to provide an information sensitivity categorization scheme allows for organizational staff to determine sensitivity using their own guidelines and judgment, which may vary widely. A consistently applied sensitivity categorization scheme also ensures consistent handling of information assets across the organization and with external entities.

Sensitivity categorization is a characteristic of an information asset that should be documented as part of the information asset inventory. *(See ADM:SG1.SP2 in the Asset Definition and Management process area.)*

Typical work products

1. Information asset sensitivity categorization scheme
2. Information asset sensitivity categorization
3. Information asset handling procedures and guidelines

Subpractices

1. Develop an information asset sensitivity categorization scheme.

   The sensitivity categorization scheme is unique to the organization and should cover all categories of information assets. The categorization levels should be appropriately defined and communicated and integrated with information asset handling and labeling procedures.

   These are examples of information asset sensitivity categorization levels:

   - unclassified, which typically includes
     - public or non-sensitive (information that is approved for public use)
     - restricted or internal use only (memos, project plans, audit reports)
     - confidential or proprietary (organizational intellectual property, product designs, customer information, employee records)
   - classified, which may include levels such as
     - secret
     - top secret

2. Assign responsibility for the assignment of sensitivity categorization levels to information assets.

   All staff who handle information assets (including those who are external to the organization) should be trained in the organization's sensitivity categorization scheme and be authorized to assign a categorization level. Training should also be provided for proper handling of each category of information asset.

3. Assign sensitivity categorization levels to information assets.

   This practice typically occurs when the information asset is defined. The categorization level should be kept as part of the definition of the information asset in the asset inventory.

4. Establish policies for proper handling of information assets according to the sensitivity categorization scheme.

5. Establish policies and procedures for proper labeling for each category of information asset.

KIM:SG2 Protect Information Assets

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

Information assets are typically some of the most vulnerable assets of the organization. Information assets come in many different forms, are often under-appreciated, and may be highly intangible (such as the knowledge of staff). Information assets are also subject to the entire range of resilience requirements—information must often be limited to those with proper authorization (confidentiality), must be reliable and usable in the form intended (integrity), and must be made available when needed to support vital services (availability).

Protecting information assets from vulnerabilities, threats, and risks requires that the organization develop appropriate resilience requirements for these assets and follow through with the development, implementation, and management of an appropriate level of administrative, technical, and physical controls to manage the conditions that could

cause disruption of these assets. The organization selects and designs controls based on the information asset's resilience requirements and the range of media on which the information asset resides (paper, electronic files, etc.). The effectiveness of these controls is monitored on a regular basis to ensure that they meet the information asset's resilience requirements.

KIM:SG2.SP1 Assign Resilience Requirements to Information Assets

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

Resilience requirements form the basis for the actions that the organization takes to protect and sustain information assets. These requirements are established commensurate with the value of the asset to services that it supports. The resilience requirements for information 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.

Resilience requirements for information assets are developed in the Resilience Requirements Development process area. However, information asset resilience requirements may not be formally defined, or they may be assumed based on the acquisition of information assets. These requirements may be under management but not formally associated with information assets. Thus, the assignment of these requirements is necessary as a foundational step for controls management.

Typical work products

1. Information asset resilience requirements

Subpractices

1. Assign resilience requirements to high-value information assets.
2. Document the requirements (if they are currently not documented) and include them in the asset definition.

KIM: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 and sustains the essential operation of information assets commensurate with their role in supporting essential organizational services. Controls are essentially the methods, policies, and procedures that the organization uses to protect and sustain high-value assets at an acceptable level. They typically fall into three categories: administrative (or managerial), technical, and physical. This is necessary particularly for information assets because they come in so many different forms and are pervasive across the organization.

- Administrative controls (often called “management” controls) ensure alignment to management’s intentions and include such artifacts as governance, policy, monitoring, auditing, separation of duties, and the development and implementation of service continuity plans.
- Technical controls are the technical manifestation of protection methods for information assets. Most prominently, they include electronic access controls, but they can also include such hardware devices as firewalls. By far, technical controls are the most pervasive type of protective controls and are often associated with security activities.
- Physical controls prevent the physical access to and modification of information assets. These controls typically include devices such as card readers on file room doors and other physical barrier methods.

Typical work products

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

Subpractices

1. Establish and implement administrative controls for information assets.

   Administrative controls for protecting information assets include

   - information security policies that govern the behavior of users, including
     - policies for the proper sensitivity categorization of information assets
     - policies for the proper disposition of information assets
     - policies for the proper backup and archiving of information assets
     - policies for the removal of information assets from the workplace
   - training to ensure proper information 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 *(See the Monitoring process area.)*
   - governance over the proper use and distribution of information, and the protection of information assets *(See the Enterprise Focus process area.)*
   - development, testing, and implementation of service continuity plans, including information asset recovery and restoration *(See the Service Continuity process area.)*

2. Establish and implement technical controls for information assets.

   Technical controls include such controls as

   - access controls for systems, databases, files, and other electronic forms of information, including user and privilege management and access management (via passwords, etc.)
   - automated backup, retention, and recovery of information assets
   - modification controls that prevent unauthorized modification and that log and report modification actions by authorized individuals

3. Establish and implement physical controls for information assets.

   Physical controls for protecting information assets include such controls as

- clean desk and clean screen policies
- physical access controls on file rooms and work areas where paper and technical information assets are stored
- facility controls that notify staff when non-employees are on the premises

4. 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.)*

KIM:SG3 Manage Information Asset Risks

Operational risks to information assets are identified and managed.

The management of risks to information assets is the specific application of risk management tools, techniques, and methods to the information assets of the organization. Because of their pervasiveness across the organization and the various forms in which they can be found, there are many opportunities for information assets to be threatened and for risk to be realized by the organization. Risks to information assets can result in consequences to the organization, including the disruption of high-value services due to the lack of information integrity and availability.

Managing information asset risks involves determining the places where information assets "live"—where they are stored, transported, or processed—typically called "containers." It is at these points where vulnerabilities and threats to information assets arise and where controls must be implemented to protect the assets from disruption or misuse. These containers include technology, physical constructs, and even people who have knowledge or information that can be disclosed or made unavailable when needed for high-value services.

KIM:SG3.SP1 Identify and Assess Information Asset Risks

Risks to information assets are periodically identified and assessed.

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

The identification of information 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. Information asset risk statements, with impact valuation
2. List of information asset risks, with categorization and prioritization

Subpractices

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

Determining which information assets to include in regular risk management activities depends on many factors, including the value of the asset to the organization and its resilience requirements.

2. Identify risks to information assets.

   Identification of risk for information assets requires an examination of where these assets are stored, transported, and processed. These places could be internal or external to the organization. Operational risks should be identified in this context so that mitigation actions are more focused and directed. Typical information asset containers include

   - technical containers, such as information systems or hardware such as servers, network segments, or personal computers
   - physical containers, such as paper, file rooms, storage spaces, or other media such as CDs, disks, flash drives
   - people, including those who might have detailed knowledge about the information asset

   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 information assets.
4. Categorize and prioritize risks to information assets.

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

5. Develop a risk disposition strategy for each information 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.

KIM:SG3.SP2 Address Information Asset Risks

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

The response to information 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 information assets, minimizing exposure to these risks, developing service continuity plans to keep the information assets viable during times of disruption, and developing recovery and restoration plans to address the consequences of realized risk.

Risk response for information assets requires the development of risk strategies and plans (which may include the development of new or revision of existing information asset controls) and to implement and monitor these plans for effectiveness.

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

Typical work products

1. Information asset risk response plans
2. List of those responsible for addressing and tracking risks
3. Status on information asset risk response plans

Subpractices

1. Develop and implement risk response plans for all risks that have a "mitigate" disposition.
2. Validate the risk response plans by comparing them to existing strategies for protecting and sustaining information 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.

KIM:SG4 Manage Information Asset Confidentiality and Privacy

The confidentiality and privacy considerations of information assets are managed.

Confidentiality and privacy are fundamental resilience requirements for information assets. These requirements are unique to information assets because the inadvertent or intentional disclosure of information to unauthorized staff can result in significant consequences to the organization, including reputation damage, harmful effects to customers and stakeholders (such as identity theft), and legal and financial penalties.

Typically, breaches of the confidentiality and privacy requirements do not directly result in disruption of associated services. Instead, because of the nature of the consequences of the breach, the disruption typically occurs at the enterprise or organizational level, and this in turn has a negative impact on one or more operational services. Thus, while the damage is referential, there is still an impact on operations that must be managed.

The development, implementation, and management of appropriate controls can limit potential breaches of confidentiality and privacy and minimize impact on operational services. These controls include encryption of data and information, controlling access to these assets, and controlling how these assets are disposed of after their useful life.

General controls relative to preserving the confidentiality and privacy of information assets may be included as part of practice KIM:SG2.SP2. However, the specific practices contained in KIM:SG4.SP1 through KIM:SG4.SP3 are targeted baseline controls that must be implemented to manage the confidentiality and privacy aspects of information assets that affect operational resilience.

KIM:SG4.SP1 Encrypt High-Value Information

Cryptographic controls are applied to information assets to ensure confidentiality and prevent accidental disclosure.

Encryption provides an additional layer of control over information assets by ensuring that they are accessible only by those who have the appropriate "keys" to decipher them. In addition to access controls, encryption provides another layer of protection because the information that is accessible is useless to anyone who does not hold the privilege of having the keys necessary to read it.

Encryption is an especially important control for information assets that are frequently transmitted electronically via networks, for media that are mobile (such as disks), and for public or private communications segments.

Encryption is typically applied to electronic forms of information assets, such as files, databases, and other media. However, paper-based information may also be encrypted (using codes) so that it is rendered meaningless to those who do not have the means to manually decipher it.

Typical work products

1. Policy and guidelines for encryption application
2. Encryption methodologies and technologies
3. Cryptographic key management policies and procedures
4. Encrypted information assets

Subpractices

1. Establish an organizational policy addressing the proper use of encryption and cryptographic means for protecting information assets.

   Encryption policies should relate to the use of cryptographic technologies that are appropriate or required for each level of information asset sensitivity categorization.

2. Establish a list of acceptable cryptographic technologies preferred by the organization.

   The use of cryptographic technologies requires organizational processes for managing the assignment, use, storage, disposal, and protection of cryptographic keys (such as public and private keys). There must be physical protection controls in place for the cryptographic infrastructure (servers, networks, etc.) so that the encryption process is not compromised, thereby reducing the effectiveness of encryption technologies.

3. Encrypt information assets based on policy and information asset sensitivity categorization.

KIM:SG4.SP2 Control Access to Information Assets

Access controls are developed and implemented to limit access to information assets.

Controlling access to information assets is a front-line defense for ensuring that these assets are provided only to authorized staff. Access controls can be electronic (i.e., implemented and enforced through user IDs, passwords,

and application system or technical infrastructure access control methodologies) or physical (placing files in rooms with card readers, putting files in locked desk drawers, implementing clean desk and clean screen policies). The organization must decide upon the right mix of controls to address the various forms of information assets and any special considerations of the assets.

Typical work products

1. List of information assets requiring access control
2. Documented access controls for information assets

Subpractices

1. Identify the information assets to which access must be controlled.

   Information assets to which access must be controlled are identified through analysis of their resilience requirements for confidentiality. Based on these requirements, the organization should prioritize information assets and determine the appropriate levels of access controls to satisfy resilience requirements. *(The selection, implementation, and management of access controls are performed in the Access Management process area.)*

   In addition, information assets that have special confidentiality and privacy considerations required by rules, laws, and regulations must be prioritized for access controls. *(Managing compliance with these rules, laws, and regulations is addressed in the Compliance process area.)*

   Examples of laws and regulations concerning confidentiality and privacy include

   - Family Educational Rights and Privacy Act (FERPA)
   - Health Insurance Portability and Accountability Act (HIPAA)
   - Gramm-Leach-Bliley Act (GLBA)
   - Fair Credit Reporting Act (FCRA)
   - Children's Online Privacy Protection Act (COPPA)

2. Develop and implement access controls to satisfy confidentiality- and privacy-related resilience requirements.

   These controls must consider and address

   - various forms in which the information asset exists (paper, electronic files, CDs, microfiche, etc.)
   - places where the asset lives (on staff members' desks, in fax machines, in file rooms, on servers, across networks, on portable media, etc.)
   - rules, laws, and regulations to which the asset is subject
   - the information asset's resilience requirements (which presumably would consider how the asset is used and its value to the organization)
   - use of the information by staff external to the organization or not under the organization's direct control
   - the information asset's sensitivity categorization

3. Manage access controls on an ongoing basis to ensure continued satisfaction of confidentiality- and privacy-related resilience requirements.

KIM:SG4.SP3 Control Information Asset Disposition

The means for disposing of information assets are controlled.

The controlled disposition of information assets is necessary to ensure that they are not disclosed to unauthorized staff. As an information asset is retired from service, it must be disposed of in a manner commensurate with its resilience requirements and sensitivity categorization, and in accordance with any applicable rules, laws, and regulations.

Proper disposition of information assets is highly dependent on the type of asset, its form, its sensitivity categorization, and other factors such as whether the disposition must be logged or tracked. The organization must develop specific guidelines to address a range of disposition issues and address them through provision of proper disposition methods such as the use of shredders or incineration.

Typical work products

1. Information asset disposition guidelines

Subpractices

1. Develop and implement guidelines for the appropriate disposition of information assets.
2. Communicate these guidelines to all staff who are responsible for the resilience of information assets.

KIM:SG5 Manage Information Asset Integrity

The integrity of information assets to support high-value services is managed.

To be usable for the purposes intended in supporting high-value services, information 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)

Information integrity provides a level of reliability that is required for the continued support of high-value services. When this integrity is violated—through unauthorized, inappropriate, or even unintentional modification of an information asset—the usability of the information asset is reduced because of real or perceived devaluation of its reliability. The consequences of improper or unauthorized modification of an information asset are vast—service delivery may be affected, operational and organizational decisions may be impeded, and the organization may suffer reputation damage, fines, legal penalties, or even the loss of life of staff, customers, or business partners as a result.

Managing information asset integrity involves controlling modification to these assets, performing configuration management, and periodically verifying the continued validity of the assets.

KIM:SG5.SP1 Control Modification of Information Assets

The modification of information assets is controlled.

Controlled modification of information assets by authorized staff ensures the continued integrity of these assets for their intended purposes. A simple way of controlling modification is to control access to these information assets—either electronically (via controlling access to networks, servers, application systems, and databases and files) or physically (by limiting access to file rooms, work areas, and facilities).

In addition to access controls, information assets can be protected from unauthorized modification by limiting the ways in which the information assets can be accessed. For example, information assets are typically modified through authorization-controlled gateways such as network and server directories or through the access control mechanisms of information systems. However, information assets are often directly modified—through direct access to a file or database or by altering information written on a paper file. By limiting the types and number of access points, the organization can also control how information assets are modified.

For effectiveness, the organization must thoroughly consider which staff are authorized to make modifications to information assets (based on the unique integrity requirements of each information asset) and implement electronic and physical controls to meet these requirements. However, because access controls are not infallible, the organization must also be able to deploy detective controls that allow for logging of information asset modification and periodic review of these logs for anomalies.

The subpractices included in this practice are generically addressed in the Access Management process area.

Typical work products

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

Subpractices

1. Establish organizationally acceptable tools, techniques, and methods for modifying information assets.
2. Identify and document staff who are authorized to modify information assets, relative to the assets' integrity requirements.

   This information may be specifically included as part of the information assets' resilience requirements.
3. Implement tools, techniques, and methods to monitor and log modification activity on high-value information assets.
4. Perform periodic audits of information asset modification logs and identify and address anomalies.

This activity may require the organization to restore information assets to an earlier version to reverse any unauthorized modification or alteration that is detected on audit logs. *(See KIM:SG5.SP2 for configuration control practices.)*

KIM:SG5.SP2 Manage Information Asset Configuration

Information asset baselines are created and changes are managed.

Establishing an information asset baseline provides a foundation for managing the integrity of assets as they change over their lifecycle. Configuration management of information assets establishes additional controls over the assets so that they are always in a form that is available and authorized for use. In this way, concerns about the validity and reliability of information assets are reduced.

Most information assets are expected to change over time—the normal course of operations will result in the creation of new information (which is essentially a modification of existing information), changes to existing information, and elimination or replacement of old or unusable information. Establishing point-in-time captures of information assets (configuration items) ensures that these assets can be restored to an acceptable form when necessary—after a disruption, when an unauthorized modification has occurred, or under any circumstances where integrity is suspect. In fact, for some assets, an organization may want to freeze a baseline information asset configuration, thus permitting no modifications or alterations to the assets over their life cycle.

Poor information asset configuration control affects the potential resilience of an information asset and the services that it supports. It also may impede the ability to execute service continuity plans that depend upon ready access to accurate and complete information.

Typical work products

1. Information asset baseline configuration
2. Configuration management policies and procedures
3. Configuration control logs and reports

Subpractices

1. Establish an information asset baseline to serve as the foundation for information asset change control.

   Remember that technical assets such as software programs can also be considered as information assets. These assets must also be included in information asset configuration management.

2. Develop and implement configuration control policies, procedures, and techniques.
3. Review configuration control logs and identify anomalies.

KIM:SG5.SP3 Verify Validity of Information

Controls are implemented to sustain the validity and reliability of information assets.

The information processing cycle—data is processed into information—is continuous. An information asset consumed in the operation of a service may exit the service as an altered asset or an entirely new asset. The alteration of information assets through the processing cycle must be controlled to ensure that the resulting information assets remain complete, accurate, and reliable. This alteration can be due to direct manipulation (such as from unauthorized access) or other operational risks (such as the loss of power during processing that results in a corrupted file or database).

There are several means by which an organization can manage potential operational risks that can affect the validity of information assets. For example:

- the use of processing "completeness" controls (which ensure that a service or a system receives complete information as expected)
- implementation of preventive controls that check for duplication of information or enforce syntax and format on information (such as acceptable formats for dates, "xx/xx/xxxx," and telephone numbers, "xxx-xxx-xxxx")
- validation of processing output, such as selecting records for recalculation or review

Typical work products

1. Information asset accuracy and completeness controls
2. Information asset validation procedures
3. Audit logs and reports

Subpractices

1. Establish requirements for the inclusion of data validation controls in services and related systems.

   The inclusion of data validation controls ensures that information assets retain their integrity when they are used in processes and systems.

2. Perform regular review of information asset output from processes.

   Validation of service and system output ensures that changes to information assets are valid, that the information assets are complete and accurate, and that the assets can continue to be used without concerns about reliability.

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

   Regularly audit and validate that information has the level of integrity required.

KIM:SG6 Manage Information Asset Availability

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

The availability of an information asset is paramount to supporting high-value services. Information may be accurate and complete, but if a service cannot use it or it isn't available on demand or in a timely matter, the service may not be able to meet its mission.

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

- the accidental or intentional alteration or modification of an information asset (which renders the information unavailable due to its resulting lack of quality and reliability)
- the destruction or loss of information due to a natural disaster such as a flood
- failure of a system disk drive or file sharing software
- failures of personal computers
- loss of paper files, CDs, and flash drives

Fortunately, information assets are often able to be cost-effectively duplicated and stored. Through proper configuration management and strong information asset retention and backup processes, organizations may find that the availability of information is controllable, even in light of a range of potential operational risks. However, this is less true of information assets that have not been formally recorded or are not easily duplicated, such as institutional knowledge that is retained by knowledgeable staff. This information must be claimed by the organization to ensure availability.

KIM:SG6.SP1 Perform Information Duplication and Retention

High-value information assets are backed up and retained to support services when needed.

The duplication and retention of information assets are primary controls for ensuring information asset availability. These controls must be applied not only to information assets that are critical to supporting high-value services but also to the restoration of these services when disrupted.

In addition to performing backup and retention of information assets that support services, the organization needs to address the retention and protection of its vital records—charters, articles of incorporation, customer contracts, employee records, etc. These information assets may not directly support a particular service, but they are critical to the overall continued viability of the organization and must be accessible particularly during disruptive events.

Typical work products

1. Information asset backup and retention procedures
2. Information asset repositories

Subpractices

1. Develop information asset backup and retention procedures.

   Information asset backup and retention procedures should include

   - standards for the frequency of backup and storage (which may be established and connected to the organization's configuration management of information assets) and the retention period for each information asset
   - the types and forms of information asset retention (paper, CDs, tapes, etc.)
   - the identification of organization-authorized storage locations and methods, as well as guidelines for appropriate proximity of these storage locations
   - procedures for accessing stored copies of information assets
   - standards for the protection and environmental control of information assets in storage (particularly if the assets are stored in locations not owned by the organization)
   - standards for the testing of the validity of the information assets to be used in restorative activities
   - periodic revision of the guidelines as operational conditions change

   The application of these guidelines should be based on the value of the asset and its availability requirements during an emergency, which may be indicated by a service continuity plan.

2. Back up and store information assets as prescribed and according to their availability requirements.

3. Periodically test the organization's backup and storage procedures and guidelines to ensure continued validity as operational conditions change.

   Stored information assets should be periodically tested to ensure that they are complete, accurate, and current and can be used for restorative purposes when necessary.

KIM:SG6.SP2 Manage Organizational Knowledge

The organizational and intellectual knowledge of staff is identified and documented.

The intellectual property of the organization is often tangible—that is, it can be viewed in annual reports, research documents, strategies and plans, or other physical forms. However, the organization also possesses institutional information that is less visible because it represents the knowledge of skilled, experienced people in the organization. Much of this institutional knowledge is often not documented but is vitally important to normal operations, especially in a disruptive situation. Unfortunately, the existence and tangibility of this knowledge are frequently established only during times of stress when people are needed to perform heroic actions to restore normal operating conditions.

The availability of institutional knowledge is directly tied to the availability of the people who possess it. Thus, when institutional knowledge is not captured and documented, the availability of this type of information asset is subject to the availability constraints of people. Because staff may be

personally affected during an emergency situation, their knowledge may not be attainable unless archived.

The issues of institutional knowledge also extend beyond the organization's borders—external entities may have specialized knowledge that the organization needs during times of stress that may not be available. To the extent possible, this knowledge should also be retained by the organization, even though the activities related to this knowledge have been outsourced to external vendors.

Typical work products

1. List of vital staff and related institutional knowledge
2. Documented information assets related to institutional knowledge
3. Information asset repository

Subpractices

1. Identify vital staff who may have institutional knowledge.
2. Identify information assets that may be in intangible forms.
3. Document information assets as necessary.
4. Develop and implement procedures for regular identification, capture, and revision of institutional knowledge.

   Cross-training is a form of institutional knowledge transfer. Cross-training should be considered for all vital staff as a part of identifying and documenting institutional knowledge. *(Training is addressed in the Organizational Training and Awareness process area.)*

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 Knowledge and Information Management process area.

KIM:GG1 Achieve Specific Goals

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

KIM:GG1.GP1 Perform Specific Practices

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

Elaboration:

Specific practices KIM:SG1.SP1 through KIM:SG6.SP2 are performed to achieve the specific goals of the knowledge and information management process.

KIM:GG2 Institutionalize a Managed Process

Knowledge and information management is institutionalized as a managed process.

KIM:GG2.GP1 Establish Process Governance

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

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

Subpractices

1. Establish governance over process activities.

   Elaboration:

   Governance over the knowledge and information management process may be exhibited by

   - establishing a higher level position, often the chief information officer or chief knowledge officer, responsible for the resilience of the organization's information assets and institutional knowledge
   - developing and publicizing higher level managers' objectives and requirements for the process
   - oversight over the management of the confidentiality, integrity, availability, and privacy of information assets
   - sponsoring and providing oversight of policy, procedures, standards, and guidelines for the documentation of information 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 the systems that store, transmit, and process information assets
   - sponsoring and funding process activities
   - providing guidance for prioritizing information assets and institutional knowledge relative to the organization's high-priority strategic objectives
   - providing guidance on information asset sensitivity categorization and handling procedures
   - providing guidance on identifying, assessing, and managing operational risks related to information assets
   - providing guidance for resolving violations of information asset confidentiality, integrity, availability, and privacy
   - 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 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 knowledge and information management policy should address

- responsibility, authority, and ownership for performing process activities
- procedures, standards, and guidelines for
  - documenting and maintaining information asset descriptions and relevant information about asset-service relationships
  - describing and identifying information asset owners and custodians
  - categorizing information assets based on sensitivity and other defined business criteria
  - developing and documenting resilience requirements for information assets
  - establishing, implementing, and maintaining an internal control system for information assets, including access control and configuration management
  - managing information asset operational risk
  - establishing service continuity plans and procedures for information assets, including backup, retention, restoration, and archiving
  - proper disposition of information assets at the end of their useful life
  - removing information assets from the workplace
  - clean desk and clean screen policies
  - applying encryption as a control for information asset confidentiality and privacy, as well as cryptographic key management
- the association of information assets to core organizational services, and the prioritization of assets and institutional knowledge required for service continuity
- requesting, approving, and providing access to information assets to persons, objects, and entities, including type and extent of access as well as requests that originate externally to the organization *(Refer to the Access Management process area for more information about granting access [rights and privileges] to information 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

KIM:GG2.GP2 Plan the Process

Establish and maintain the plan for performing the knowledge and information management process.

Elaboration:

A plan for performing the knowledge and information management process is created to preserve the confidentiality, integrity, and privacy of information assets and to ensure that information assets and institutional knowledge remain available and viable to support organizational services. The plan must address the resilience requirements of the information assets, dependencies of services on these assets, and consideration of multiple asset owners and custodians at various levels of the organization. In addition, because information is often an intangible asset that can be stored, processed, and transmitted anywhere, the plan must extend to external stakeholders that can enable or adversely affect information asset resilience.

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 information assets, as well as duplication and retention of high-value information assets. These activities address protecting and sustaining information assets and preserve collective institutional knowledge commensurate with asset 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.

KIM:GG2.GP3 Provide Resources

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

Elaboration:

The diversity of activities required to protect and sustain information 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 perform the knowledge and information management process:

- information, application, and technical security staff, including those who establish, implement, or maintain information asset internal controls
- staff responsible for controlling modifications to information assets and verifying their continued validity and reliability
- staff involved in managing and protecting the assignment, use, storage, disposal, and protection of cryptographic keys
- business continuity and disaster recovery staff
- IT operations and service delivery staff
- privacy, security, confidentiality officer or equivalent
- staff responsible for establishing and maintaining physical security over areas where information assets are stored or processed (such as security guards)
- staff involved in operational risk management of information assets, including insurance and risk indemnification staff
- staff responsible for developing service continuity and risk response plans and ensuring they are aligned with stakeholder requirements and needs
- external entities responsible for creating, storing, processing, transmitting, duplicating, retaining, and disposing of information assets
- staff responsible for managing external entities that have contractual obligations for process activities
- owners and custodians of high-value information assets (to identify and enforce resilience requirements and support the accomplishment of operational resilience management objectives)
- internal and external auditors responsible for reporting to appropriate committees on process effectiveness

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

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

2. Fund the process.

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

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

   Elaboration:

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

   - methods, techniques, and tools for managing risks to information assets, including tracking open risks to closure and monitoring the effectiveness of information asset risk response plans
   - methods, techniques, and tools for describing and categorizing information assets and maintaining the asset inventory that contains this information

- methods, techniques, and tools for maintaining information assets, including asset configuration management and monitoring and logging of modification activities
- methods for establishing, implementing, and maintaining the internal control system for information assets
- methods, techniques, and tools for encryption and key management
- methods for the proper disposition and disposal of information assets
- methods, techniques, and tools for information asset backup, retention, recovering, and archiving
- database systems for information asset inventories and knowledge management

KIM:GG2.GP4 Assign Responsibility

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

Elaboration:

Of paramount importance in assigning responsibility for the knowledge and information management process is the establishment of information asset owners and custodians *(described in ADM:SG1.SP3)*. Owners are responsible for establishing information 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 privacy, confidentiality, integrity, and availability 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-related 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 information 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 managing information assets (including implementation and management of controls and sustaining services that use the information assets).

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

   Elaboration:

   Responsibility and authority for performing knowledge and information 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 and derive benefit from the process for assets and services 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 creating, storing, processing, transmitting, duplicating, retaining, and disposing of information assets, where applicable
- including process tasks in staff performance management goals and objectives, with requisite measurement of progress against these goals
- 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.

KIM:GG2.GP5 Train People

Train the people performing or supporting the knowledge and information 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 knowledge and information management process:

- prioritization and sensitivity categorization of information assets
- methods for eliciting, developing, and documenting information resilience requirements
- knowledge of tools, techniques, and methods that can be used to identify, analyze, mitigate, and monitor operational risks to information assets
- establishing, implementing, and maintaining the internal control system for information assets
- capturing institutional information that represents the knowledge of skilled, experienced people in the organization
- protecting and sustaining information assets to meet their resilience requirements and their confidentiality, integrity, availability, and privacy requirements

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:

   - information asset risk management concepts and activities (e.g., risk identification, evaluation, monitoring, and response)
   - information asset definition, sensitivity categorization, prioritization, and handling
   - information asset resilience requirements development
   - establishing, implementing, and maintaining internal controls for protecting and sustaining information assets
   - cross-training to support institutional knowledge transfer
   - proper techniques for information asset disposal
   - information asset configuration and change management
   - supporting information 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 knowledge information and management activities
   - using process methods, tools, and techniques, including those identified in KIM:GG2:GP3 subpractice 3
4. Provide training and review the training needs as necessary.

KIM:GG2.GP6 Control Work Products

Place designated work products of the knowledge and information management process under appropriate levels of control.

Elaboration:

KIM:SG1.SP1 and KIM:SG1.SP2 specifically address use of and updates to the information asset inventory, including the designation of information assets as high-value, information asset sensitivity categorization, and handling.

These are examples of information asset work products placed under control:

- inventory, sensitivity categorization scheme, and sensitivity categories
- information asset resilience requirements (confidentiality, integrity, availability, and privacy)
- administrative, technical, and physical controls
- list of operational risks by asset and asset sensitivity category with prioritization, risk disposition, response plans, and current status
- risk statements with impact valuation
- encryption and key management methods, techniques, and technologies
- encrypted information assets
- access control lists
- disposition guidelines
- baseline configurations and configuration control logs and reports

- information asset and institutional knowledge repositories
- backup media
- process plan
- policies and procedures
- contracts with external entities

KIM:GG2.GP7 Identify and Involve Relevant Stakeholders

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

Subpractices

1. Identify process stakeholders and their appropriate involvement.

   Elaboration:

   Because of the significant connection between information assets and the technology, facility, and people assets that store, transmit, and process the information, many of the stakeholders are likely to be external to the organization.

   These are examples of stakeholders of the knowledge and information management process:

   - owners and custodians of information assets
   - owners and custodians of technology and facility assets that are used in storing, transmitting, and processing information assets
   - service owners
   - organizational unit and line of business managers responsible for high-value information assets and the services they support
   - staff responsible for managing operational risks to information assets
   - staff responsible for establishing, implementing, and maintaining an internal control system for information assets, including those responsible for access control, configuration management, and encryption
   - staff required to develop, test, implement, and execute duplication and retention plans for information assets
   - external entities that are involved in creating, storing, processing, transmitting, duplicating, retaining, and disposing of information assets
   - staff in other organizational support functions, such as accounting or general services administration (particularly as related to information asset valuation and disposition)
   - internal and external auditors

   Stakeholders are involved in various tasks in the knowledge and information management process, such as

   - planning for the process
   - creating an information asset repository
   - creating information asset descriptions, including asset sensitivity categorization and handling
   - associating information assets with services and analyzing service dependencies
   - developing information asset resilience requirements

- assigning resilience requirements to the systems that store, transmit, and process information assets
- establishing, implementing, and managing information asset controls
- developing service continuity plans (duplication, retention, restoration, archival) for information assets
- managing operational risks to information assets
- controlling the operational environment in which information assets "live"
- managing information asset external dependencies for assets that are created, stored, processed, transmitted, duplicated, retained, and disposed of by external entities
- managing relationships with external entities that provide information 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.

KIM:GG2.GP8 Measure and Control the Process

Measure and control the knowledge and information 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 knowledge and information management process:

   - percentage of information assets that have been inventoried
   - percentage of information assets with/without a complete asset profile (such as no stated resilience requirements
   - percentage of information assets with/without a designated owner

- percentage of information assets with/without a designated custodian (if applicable)
- percentage of information assets that have designated owners but no custodians (if applicable)
- percentage of information assets that have designated custodians but no owners
- percentage of information assets that have been inventoried, by service
- percentage of information assets that are not associated with one or more services
- elapsed time since the information asset inventory was reviewed
- percentage of information asset-service dependency conflicts with unimplemented or incomplete mitigation plans
- percentage of information asset-service dependency conflicts with no mitigation plan
- number of discrepancies between the current inventory and the previous inventory
- number of changes made to asset profiles in the information asset inventory
- number of changes to resilience requirements as a result of information asset changes
- number of changes to service continuity plans as a result of information asset changes
- percentage of information assets that are designated as high-value assets
- elapsed time since review and validation of high-value information assets and their priorities
- number of information assets categorized by service (includes number of assets that support 2 or more, 3 or more, etc., services)
- percentage of information assets that have not been categorized as to level of sensitivity
- percentage of information assets without assigned/defined resilience requirements
- percentage of information assets with assigned/defined resilience requirements that are undocumented
- percentage of information assets with no (or missing) protection controls
- percentage of information assets with no (or missing) sustainment controls
- percentage of information asset controls (protection and sustainment) that are ineffective or inadequate as demonstrated by:
  - unsatisfied control objectives
  - unmet resilience requirements
  - outstanding control assessment problem areas above established thresholds and without remediation plans
- percentage of information 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 information asset controls
- elapsed time since risk assessment of information assets performed
- elapsed time since business impact analysis of information assets performed
- percentage of information assets for which business impact valuation (qualitative or quantitative) has not been performed

- percentage of information assets for which a risk assessment has not been performed and documented (per policy or other guideline) and according to plan
- percentage of information asset risks that have not been assigned to a responsible party for action, tracking, and closure
- percentage of information asset risks with a disposition of "mitigate" that do not have a defined mitigation plan
- percentage of information asset risks with a "mitigate" disposition that are not effectively addressed by their response plans
- percentage of realized risks for information assets that exceed established risk parameters
- number of violations of access control policies for information assets
- percentage of information assets for which encryption is required and not implemented
- percentage of retired information assets that are not disposed of in accordance with information asset disposition guidelines
- percentage of retired information assets that have not been disposed according to plan
- percentage of anomalies in information asset modification logs that have not been addressed as scheduled
- percentage of anomalies in information asset configuration control logs that have not been addressed as scheduled
- percentage of information asset logs which are not validated and placed under configuration control as scheduled
- percentage of information assets with accuracy and completeness controls that have not been reviewed as scheduled
- percentage of information assets that have not been backed up as scheduled
- percentage of information assets that have not been tested to verify that they can be accurately restored from backups as scheduled
- percentage of vital staff with institutional knowledge where such knowledge has not been captured/transferred (via such methods as cross training)
- percentage of information assets that do not satisfy their resilience requirements
- number of policy violations related to confidentiality, integrity, availability, privacy, and access control of information assets
- percentage of external entities that are not meeting service level agreements for information assets subject to external entity services
- percentage of information assets that are not maintained at required maintenance levels (for information assets subject to maintenance agreements)

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 information asset inventory.

Periodic reviews of the knowledge and information management process are needed to ensure that

- newly acquired information assets are included in the inventory and retired assets are deleted from the inventory
- information assets have stated resilience requirements
- information assets that have been modified are reflected accurately in the inventory
- information asset-service mapping is accurate and current
- ownership and custodianship over information assets are established and documented
- administrative, technical, and physical controls are operating as intended
- controls are meeting the stated intent of the resilience requirements
- institutional knowledge is being identified, collected, and stored
- status reports are provided to appropriate stakeholders in a timely manner
- information 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 information 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 (i.e., preventive, detective, corrective, compensating, etc.). Because of the tightly coupled nature of information and the systems that store, transmit, and process information, corrective action may also involve technology and facility asset controls.
7. Track corrective action to closure.

KIM:GG2.GP9 Objectively Evaluate Adherence

Objectively evaluate adherence of the knowledge and information 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 information assets
- identifying information asset resilience requirements
- establishing and implementing information asset controls
- identifying and managing information asset risks
- developing service continuity plans for information assets (backup, retention, restoration, archival) and the technology and facility assets where information assets are stored, processed, and transmitted
- identifying and managing information asset dependencies
- identifying and managing changes to information assets
- properly disposing of information assets at the end of their useful life
- aligning stakeholder requirements with process plans
- assigning responsibility, accountability, and authority for process activities
- determining the adequacy of process reports and reviews in informing decision makers regarding the performance of operational resilience management activities and the need to take corrective action, if any
- verifying information controls
- using process work products for improving strategies for protecting and sustaining information assets

These are examples of work products to be reviewed:

- information asset inventory
- information asset internal controls documentation
- information asset resilience requirements documentation
- information asset risk statements
- information asset risk response plans
- service continuity plans for information assets and the technology and facility assets where information assets are stored, processed, and transmitted
- information asset maintenance records and change logs
- business impact analysis results for information assets
- lists of key providers and contacts for information assets
- retirement standards for information assets
- process plan and policies
- information asset issues that have been referred to the risk management process
- process methods, techniques, and tools
- metrics for the process *(Refer to KIM:GG2.GP8 subpractice 2.)*
- contracts with external entities

KIM:GG2.GP10 Review Status with Higher Level Managers

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

Elaboration:

Status reporting on the knowledge and information 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 information 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.

KIM:GG3 Institutionalize a Defined Process

Knowledge and information management is institutionalized as a defined process.

KIM:GG3.GP1 Establish a Defined Process

Establish and maintain the description of a defined knowledge and information management process.

Elaboration:

Knowledge and information management tends to be tightly coupled with the systems that store, transmit, and process the information. Due to this coupling, knowledge and information 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 information, technology, and facility assets). However, to achieve consistent results in creating and managing information assets, the activities at the organizational unit or line of business level must be derived from an enterprise definition of the knowledge and information management process. The information 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 information 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 information 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 knowledge and information 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.

KIM:GG3.GP2 Collect Improvement Information

Collect knowledge and information 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:

- information asset inventories
- inventory inconsistencies and issues
- reports on the effectiveness and weaknesses of controls
- improvements based on risk identification and mitigation
- effectiveness of information asset service continuity plans (and supporting technology and facility asset service continuity plans) in execution
- metrics and measurements of the viability of the process *(Refer to KIM:GG2.GP8 subpractice 2.)*
- changes and trends in operating conditions, risk conditions, and the risk environment that affect process results
- lessons learned in post-event review of information asset incidents and disruptions in continuity (including confidentiality, integrity, availability, and privacy)
- maintenance issues and concerns for information assets
- conflicts and risks arising from dependencies on external entities
- lessons learned in backing up, retaining, restoring, archiving, updating, and disposing of information assets
- resilience requirements that are not being satisfied for information 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.