Software Engineering Institute

CERT® Resilience Management Model, Version 1.2

Environmental Control (EC)

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

February 2016

CERT Program
Unlimited distribution subject to the copyright.

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

Carnegie Mellon

Copyright 2016 Carnegie Mellon University

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

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

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

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Internal use:* Permission to reproduce this material and to prepare derivative works from this material for internal use is granted, provided the copyright and "No Warranty" statements are included with all reproductions and derivative works.

External use:* This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other external and/or commercial use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

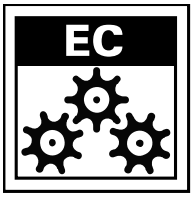
* These restrictions do not apply to U.S. government entities.

Carnegie Mellon® and CERT® are registered marks of Carnegie Mellon University.

DM-0003234

ENVIRONMENTAL CONTROL

Operations



Purpose

The purpose of Environmental Control is to establish and manage an appropriate level of physical, environmental, and geographical controls to support the resilient operations of services in organizational facilities.

Introductory Notes

Facilities are a subset of the physical plant assets of the organization that are relied upon to execute a service. They are hubs of activity where many of the organization's services intersect, such as office buildings and warehouses. Facilities can be owned by the organization but just as often are leased from an external provider, and they may even encompass workers' homes and other locations where high-value services are physically executed.

People, information, and technology assets "live" within a physical facility—they provide the physical space for the actions of people (people work in offices), the use and storage of information (such as in file rooms and on servers), and the operation of technology components (such as in data centers and server farms). Because of its nature as an activity hub, when a facility is disrupted, there is often a widespread cascading effect on the operability of these other assets, impacting mission assurance of associated services and possibly translating to a failure to achieve organizational goals and objectives.

As a complicating factor, organizations frequently execute their services in facilities that they do not own or control. These arrangements sometimes also mean that the organization's assets are co-located with the assets of other organizations. This presents challenges not only for facilities management but for ensuring the operational resilience of services that depend on these facilities to meet their missions.

The Environmental Control process area addresses the importance of facilities in the operational resilience of services as well as the unique issues that facility assets inherit because of their geographical location and the environment in which they operate. In this process area, facility assets are prioritized according to their value in supporting high-value organizational services. Physical, technical, and administrative controls that sustain the operational viability of facility assets are selected, implemented, and managed, and the effectiveness of these controls is monitored. In addition, facility risks are identified and addressed in an attempt to prevent disruption where possible. Because a facility is intricately tied to the geographical location in which it operates, the unique dependencies of the facility on its adjacent environment are identified and actively managed.

Related Process Areas

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

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

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

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

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

The development of service continuity plans for facilities 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
EC:SG1 Establish and Prioritize Facility Assets	EC:SG1.SP1 Prioritize Facility Assets
	EC:SG1.SP2 Establish Resilience-Focused Facility Assets
EC:SG2 Protect Facility Assets	EC:SG2.SP1 Assign Resilience Requirements to Facility Assets
	EC:SG2.SP2 Establish and Implement Controls
EC:SG3 Manage Facility Asset Risk	EC:SG3.SP1 Identify and Assess Facility Asset Risks
	EC:SG3.SP2 Address Facility Risks
EC:SG4 Control Operational Environment	EC:SG4.SP1 Perform Facility Sustainability Planning
	EC:SG4.SP2 Maintain Environmental Conditions
	EC:SG4.SP3 Manage Dependencies on Public Services
	EC:SG4.SP4 Manage Dependencies on Public Infrastructure
	EC:SG4.SP5 Plan for Facility Retirement

Specific Practices by Goal

EC:SG1 Establish and Prioritize Facility Assets

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

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

In many cases, all facility assets may be considered of high value to the organization. However, from a risk and resilience perspective, these assets must be prioritized. Prioritization establishes the facility assets that are of most value to the organization (based on their support for high-value services) and for which protective controls and sustainability measures are required. Failure to prioritize facility assets may lead to inadequate operational resilience of high-value assets and excessive levels of operational resilience for non-high-value assets.

EC:SG1.SP1 Prioritize Facility Assets

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

The prioritization of facility assets must be performed in order to ensure that the organization properly directs its operational resilience resources to the assets that most directly contribute to the services supporting 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.

Facility asset prioritization is performed relative to related services—that is, facility 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 facility assets, such as the following:

- the use of the facility asset in the general management and control of the organization (corporate headquarters, primary data centers, etc.)
- facility assets that are important to supporting more than one service
- the 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 facility asset and continue to meet its mission

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

Typical work products

1. List of high-value facility assets

Subpractices

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

   Facilities assets that are essential to the successful operation of organizational services should be included on the list of facility assets. *(An inventory of high-value facilities 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.

   These are examples of high-value facilities:

   - office buildings (such as the headquarters building or a branch office)
   - manufacturing facilities (such as manufacturing plants)

- data centers and other processing centers (such as call centers, payment processing locations)
- physical plants (such as telecommunications hubs)
- other physical structures where significant people, information, or technology assets exist (such as off-site data storage centers and SCADA operation centers)

2. Prioritize facility assets.

   The prioritization of facility assets is necessary so that the organization can ensure it focuses protection and sustainability activities on facilities that have the most potential for impacting the organization if they are disrupted or destroyed.

   Unlike other organizational assets, facilities tend to be "hubs" of services; that is, many services tend to be performed in or supported by a single facility. An example of this would be a data center where many application systems (and their associated hardware, software, and network components) support a number of organizational services. Because the loss of a facility can have widespread cascading effects on a number of services, the organization should consider this strongly when prioritizing facility assets. One means for supporting this criterion is to review the mapping between services and facility assets. *(The association of services to facility assets is performed in practice ADM:SG2.SP1 in the Asset Definition and Management process area.)* This information may also be gathered as the result of a business impact analysis activity at the organizational unit level.

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

EC:SG1.SP2 Establish Resilience-Focused Facility Assets

Facility assets that specifically support the organization's service continuity plans are identified and established.

Some facility assets are specifically designated to support the organization's ability to execute service continuity plans. They provide physical locations where people can work temporarily, information can be stored and retrieved when needed, and technology components such as systems, hardware, and software can be operated. In many cases, resilience-focused assets may be owned by the organization (i.e., the organization may have a secondary data center) or may be contracted for and provided by an external provider (such as the use of a shared data center to recover systems and networks).

A resilience-focused asset may also serve as a primary facility that has been designated as a recovery site during an incident. For example, an organization may have two geographically dispersed data centers where day-to-day processing occurs; however, when an incident affects one of the data centers, the other is capable of being used to support operations of the other for a specified time period. When this occurs, primary facilities also are designated as resilience facilities, increasing the need for protection and sustainability.

Typical work products

1. List of resilience-focused facility assets

Subpractices

1. Compile a list of resilience-focused facility assets from the organization's asset inventory.

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

2. Periodically reconcile the list of resilience-focused facilities to the organization's service continuity plans and resilience-focused strategies.

EC:SG2 Protect Facility Assets

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

Facility assets are one of the most tangible and visible assets of the organization. They provide a physical presence to the organization and are the intersection point for people, processes, and technologies that fuel organizational services. Thus, the availability of facilities is important to the viability of organizational services—an organization has only to close an office building for one day to realize that many job functions go unperformed during such a disruption, no matter the cause.

Facility assets present unique challenges for managing operational resilience. Facility assets are often leased from external business partners, and therefore the organization may not have direct control or influence over their protection or sustainability. Facility assets also often take non-traditional forms. For example, in a distributed workforce employees may work at home, whereby their home location becomes an extension of the organization's physical plant.

Facility assets are also uniquely connected to their immediate environment in that their operational resilience is often dependent on the resilience of public services (police, fire, ambulance, and first responders) and infrastructure (electricity, gas, water, telecommunications). Because organizations have very little if any control over the immediate environment, managing operational resilience for facilities may require extensive considerations of redundancy, co-location, geographical dispersion, etc.

Protecting facility 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 facility asset's resilience requirements and the conditions that require availability of the facilities. The effectiveness of these controls is monitored on a regular basis to ensure that they meet the facility asset's resilience requirements.

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.

EC:SG2.SP1 Assign Resilience Requirements to Facility Assets

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

Resilience requirements form the basis for the actions that the organization takes to protect and sustain facility assets. These requirements are established commensurate with the value of an asset to services that it supports. The resilience requirements for facility 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 facility assets are developed in the Resilience Requirements Development process area. However, facility asset resilience requirements may not be formally defined, or they may be assumed to be the responsibility of the facility asset owner (if the organization is not the owner). The assignment of these requirements is necessary as a foundational step for controls management.

Typical work products

1. Facility asset resilience requirements

Subpractices

1. Assign resilience requirements to facility assets.

   Resilience requirements for a facility asset are likely to be concentrated on the availability of the facility. The requirements must take into consideration the shared use of the facility both within the organization (as more than one service is likely to be performed in the facility) as well as outside of the organization (as a leased facility may be shared with other organizations that have differing resilience requirements).

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

EC: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 facility assets commensurate with their role in supporting organizational services. Controls are the methods, policies, and procedures that the organization uses to provide an acceptable level of protection over high-value assets such as facilities. These controls typically fall into three categories: administrative (or managerial), technical, and physical, the latter of which is most typically associated with facilities.

- Administrative controls (often called “management” controls) ensure alignment to management’s intentions and include such work products as governance, policy, training and awareness, pre-employment screening, and the development and implementation of service continuity plans. Administrative controls for facilities include policies on who can enter facilities, when, and under what conditions or criteria.

- Technical controls are the technical manifestation of protection methods for facility assets. Most prominently, they include access controls such as card-controlled entry gates and appropriate lighting or fencing, but they can also include such hardware artifacts as encryption.
- Physical controls manage the physical access to facility assets. These controls typically include artifacts such as picture IDs, locks on file room doors, and other physical barrier methods. By far, physical controls are the most pervasive type of protective controls applied to facilities and are often associated with security activities.

Operational resilience for facilities involves a thorough consideration of several types of controls. These include not only access controls but controls that address the viability and operability of a facility in its geographical location and immediate environment. Because most facilities aren't portable (in contrast with information assets and some technology assets), controls that prevent facilities from being impacted by vulnerabilities and threats in their immediate environment must be considered and implemented.

Typical work products

1. Facility asset administrative controls
2. Facility asset technical controls
3. Facility asset physical controls
4. List of required controls over the design, leasing, co-location, or construction of facility assets

Subpractices

1. Establish and implement administrative controls for facility assets.

Administrative controls for protecting facility assets include

- policies and standards for providing access to facilities
- standards for facility site selection, construction, and management (addressing issues of co-location, geographical dispersion, proximity, etc.)
- availability of adequate utility and communications providers
- relevant health and safety regulations and standards
- hiring procedures, particularly where they apply to physical security staff such as security guards
- evacuation procedures
- fire suppression and handling procedures
- procedures for handling events such as hardware failure, bomb threats, and loss of electrical power, water, or other utilities
- resilience training and awareness
- logging, monitoring, and auditing controls to detect and report unauthorized access and use of facilities *(See the Monitoring process area.)*
- development, testing, and implementation of service continuity plans, including facility asset substitution or restoration *(See the Service Continuity process area.)*

2. Establish and implement technical controls for facility assets.

Technical controls include such controls as

- access controls, such as
  - electronic key pads, card readers, and other electronic authenticators
  - "mantraps"
  - biometric authenticators
  - access logging and monitoring systems
- application systems for managing and controlling physical access
- environmental monitoring and control systems (particularly for data centers)
- inventory tracking and monitoring (via RFID or other technology)
- systems for monitoring viability of public services such as electricity, gas, water, and telecommunications
- direct connection alarm systems that report to public authorities

3. Establish and implement physical controls for facility assets.

Physical controls for protecting facility assets include such controls as

- physical barrier controls around a facility, including barriers and gates
- physical security buffers
- external doors suitably protected with control mechanisms such as bars, alarms, and locks
- staffed reception areas or other means to control physical access
- clean desk and clean screen policies
- physical access controls on file rooms and work areas
- intruder detection systems to cover all doors, windows, unoccupied areas, etc., including motion detectors and visual monitoring and recording
- facility controls that notify staff when non-employees are on the premises

4. Establish and specify controls over the design, construction, or leasing of facility assets.

A specific subset of controls should be considered during the design, construction, or leasing of facility assets. These controls are typically technical or physical in nature and are focused on sustaining the operability and viability of facilities, thus contributing to a facility's operational resilience.

When designing, constructing, or acquiring a facility, the following controls should be considered:

- secured facility site—buildings should be unobtrusive and give minimum indication of their purpose, with no obvious signage
- geographical location—proximity to climatic, geological, and hydrological events
- environmental conditions—dust, vibration, noise, electrical supply interference, communications interference, electromagnetic radiation
- availability of support utilities—water, sewage, electricity, heating/ventilation, air conditioning
- business factors—educated and skilled workforce, tax incentives, insurance costs
- walls—fire rating, load, floor-to-ceiling barrier, reinforcement for use in secured areas

- partitions—considerations similar to those for walls, plus the requirement of extension above dropped ceilings and below raised floors
- doors—fire rating, directional opening, resistance to being forced open, intrusion detection alarms, type of locks
- windows—characteristics of window material, intrusion detection mechanism, placement of windows
- ceiling—fire rating, load, waterproof (especially in shared tenant facilities), drop ceiling
- floor—fire rating, load, raised floor, electrical grounding, non-conductive material
- heating, ventilation, air conditioning (HVAC)—power source, protected intake vents to prevent tampering, emergency power off, air pressure, specialized chilling and cooling for technical equipment
- power supplies—backup or redundant power supply, clean power supply, circuit breakers, access to power distribution panels, emergency power off
- liquid and gas lines—accessible shutoff valve, positive flow, leakage sensor, placement of liquid and gas lines
- fire detection and suppression—fire or smoke detector and alarm, gas discharge system, placement of detectors and sprinkler heads
- emergency lighting—essential power supply and battery for emergency lighting
- moisture—water or liquid detection and alarm
- cables and cableways—routing, protection from fire, moisture, and unauthorized access

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.*

EC:SG3 Manage Facility Asset Risk

Operational and environmental risks to facility assets are identified and managed.

The management of risk for facility assets is the specific application of risk management tools, techniques, and methods to the facility assets whether or not they are owned by the organization. Facility assets are more prone to certain types of operational risk, particularly external conditions such as failures of public infrastructure and natural disasters. In addition, because facility assets are often not in the direct control of the organization (because they are leased or shared), the organization may be exposed to additional risks that would generally be detectable and controllable if the organization owned and maintained them. As hubs of activities and services, facility assets are subject to risks that can result in widespread and cascading consequences to the organization.

EC:SG3.SP1 Identify and Assess Facility Asset Risks

Risks to facility assets are periodically identified and assessed.

Operational risks that can affect facility 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. Special attention should be given to operational risks such as

natural disasters and environmental conditions to which facilities are typically prone.

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

Subpractices

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

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

2. Identify risks to facility assets.

   Identification of risk for facilities requires an examination of the types of threats, vulnerabilities, events, or incidents to which the facility may be subjected. The types of events or incidents that could occur at a given facility may be based on the history of previous events at that site or a similar site, events that may be common to the type of service, or natural disasters particular to certain geography. Operational risks should be identified in this context so that response actions are more focused and directed. Types of facility asset threats, vulnerabilities, events, and incidents to consider may include

   - non-criminal events such as human-made and natural disasters
   - crime-related events such as theft, trespassing, and sabotage
   - the demographic/social/political climate in which the facility is located
   - geographical proximity to other high-value organizational facilities
   - people, including those who might have detailed knowledge about the facility 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 facility assets.
4. Categorize and prioritize risks to facility assets.

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

5. Develop a risk disposition strategy for each facility 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.

EC:SG3.SP2 Address Facility Risks

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

Addressing facility 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 facility assets, minimizing exposure to these risks, developing service continuity plans to keep the asset viable during times of disruption or to provide a suitable substitute facility, and developing recovery and restoration plans to address the consequences of realized risk. In the case of facility assets, restoration may be a more extensive consideration—for example, restoration may mean that a new facility must be constructed or acquired, therefore recovery operations in a temporary or leased facility may be needed for a longer period of time. This temporary arrangement can also bring additional risk to the organization that must be addressed until restoration has been accomplished.

Addressing risk to facility assets requires the development and implementation of risk response plans (which may include the development of new or revision of existing facility asset controls) and the monitoring of 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. Facility asset risk response plans
2. List of those responsible for addressing and tracking risks
3. Status on facility asset risk response plans

Subpractices

1. Develop and implement risk mitigation plans for all risks that have a “mitigate” or “control” disposition.
2. Validate the risk response plans by comparing them to existing protection and sustainability strategies.
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.

   Service continuity plans that involve the use of temporary or leased facilities while restoration can be completed for a facility may result in residual risk. This risk should be characterized and addressed in the risk management cycle if necessary.
5. Implement the risk response plans and provide a method to monitor the effectiveness of these plans.
6. Monitor risk status.
7. Collect performance measures on the risk management process.

EC:SG4 Control Operational Environment

The operational environment of the facility is controlled to ensure its availability.

The *availability* of a facility—the most important challenge for the operational resilience of facilities—is dependent on several factors. First, the facility must provide access to people (both inside and outside of the organization) who need to use it to perform their job responsibilities *and* prevent access from those who do not have a legitimate need. Second, the facility must be operationally viable—it must be structurally sound, fit for purpose, and connected to vital services such as electricity, water, and telecommunications. Finally, availability of a facility is tied to its geographical location. Any event that affects the surrounding environment of the facility can impede access (and egress to some extent).

Certain operational risks, such as the following, can significantly affect the availability of a facility in supporting high-value services:

- Electronic or physical access systems can be compromised, allowing unauthorized access that may affect the availability of the facility (particularly if it is destroyed in some way) or preventing access by authorized individuals.
- Geographical events specific to the facility can occur, including hurricanes, tornadoes, winter storms, and other natural events.
- Sociopolitical events can prevent people and business partners from accessing the facility because of dangerous conditions or because of perceived danger (such as when a bomb threat is issued).
- The systems and the structures of the facility can fail, thereby rendering the facility unusable for a period of time.
- The public infrastructure that the facility depends upon can fail, thereby causing the facility to be unusable for a period of time.
- Business partners (who own or manage facilities that the organization leases or shares with other organizations) may fail to ensure the availability of their facilities, thereby posing cascading risks to the organization.

Unfortunately, facilities cannot be easily duplicated or replicated, so ensuring their availability (or more important, preserving their ability to support high-value services) is problematic. In addition, because facilities are high-cost assets, strategies for ensuring their availability are often more difficult and costly than those that are focused on information assets, technology, and in some cases, people.

To effectively control the operational environment for facilities, the organization must perform several activities. Foremost, the organization must plan for facility sustainability to ensure the continued operation of the facility (or the ability to replicate and sustain the continued operation of the facility). In addition, the organization must address the environmental conditions of the facility (to ensure that it remains viable) and consider the challenges presented by the facility's geographical environment, including its access to public and private services and infrastructure.

EC:SG4.SP1 Perform Facility Sustainability Planning

The availability of high-value facilities is ensured through sustainability planning.

Because facilities operate as hubs for services, planning for the continued operation of a facility—or in many cases, the replication of functionality at a redundant or backup facility—is a critical activity in ensuring operational resilience.

An organization has several options when performing sustainability planning for facilities. The most costly option is to construct or acquire a redundant facility that would back up an existing facility in a seamless way if disrupted. This is not always a valid option because of cost and co-location, proximity, and geographical dispersion issues. Less costly options may involve the alternate use of other organization-owned facilities (if possible) or the use of shared space (either leased space or shared services). Options that include the use of externally owned facilities bring additional risks that must be considered. Finally, instead of full facility redundancy, the organization may consider only those elements that must be made redundant (such as providing an organization-controlled source of power or telecommunications) that would render a facility usable for an acceptable specific period of time.

Facility sustainability planning is typically performed as part of developing service continuity plans for services or may be instantiated in continuity plans specifically focused on high-value facilities regardless of their use. The actions that the organization needs to take to ensure that services can be executed when facilities are disrupted are included in service continuity plans. In addition to providing facility redundancy and backup, additional issues such as “return to work” considerations may be addressed and included in facility continuity plans.

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 considerations of the practices in the Service Continuity process area have been made.

Considerations for “return to work” issues are addressed in the People Management process area.

Typical work products

1. Results of business impact analysis
2. Service continuity plans (specifically addressing facility sustainability)

Subpractices

1. Perform business impact analysis.

   Business impact analysis can help the organization to identify high-value facilities for which service continuity plans must be developed and implemented. This analysis may concentrate on reviewing the business impact of loss of services due to the loss of a facility or specifically focus on the facility itself and its associated services and the impact of their loss on the organization.

2. Develop service continuity plans that address facility availability.

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

EC:SG4.SP2 Maintain Environmental Conditions

Environmental conditions of facility assets are maintained.

The environmental condition of a facility is important for keeping it viable and operational. Failure to monitor and correct conditions may affect the availability of the facility to support the services that are convergent there. These are examples of systems that can affect environmental conditions:

- HVAC systems must be fully operational to ensure the comfort of workers as well as to keep technical equipment from overheating and failing.
- Fire suppression systems must be active to prevent fire damage and to ensure staff safety.
- Dust and air control systems must provide purified air required for production processes, particularly if "clean room" conditions are necessary.
- Power conditioning systems must condition power to ensure consistent delivery and the avoidance of "spikes."
- Security systems must be able to monitor the facility and provide authenticated access to authorized staff.
- Water systems must provide potable water for drinking purposes and other water for supporting production processes (such as for chillers for equipment and for air conditioning).

Maintaining environmental conditions includes the performance of regular maintenance activities. The criteria used to establish guidelines for maintenance are relative to the value of the related services supported by the assets that are located in the facility. The organization may use other criteria to establish guidelines for maintenance, such as

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

Typical work products

1. List of facility control equipment
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
6. Updated service continuity plans

Subpractices

1. Identify control systems that require regular maintenance in support of sustainability.
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 facility control equipment and stored appropriately with access only to authorized individuals. Risks related to control 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.

EC:SG4.SP3 Manage Dependencies on Public Services

Dependencies on public services for facility assets are identified and managed.

Because they are geographically static, facilities rely on public services that are in operation in the immediate environment in which the facilities exist. These public services may be vital to a facility's continued operation during a disruption and, by default, to the services that are performed in the facility. Thus, a thorough consideration of these services must be given for service continuity planning and incorporated into requisite service continuity plans.

Public services generally include services that are specific to the geographical region of the facility and are financed by public funds. (In some cases, depending on the organization and its size, these services may have been privatized and therefore may be financed by and under the direct control of the organization.) Public services include

- fire response and rescue services
- local and, in some cases, federal law enforcement (police, National Guard, FBI, etc.)
- emergency management services, including paramedics and first responders
- other services, such as animal control

Identifying and managing dependencies on public services may be performed as part of the organization's service continuity planning process or in the development of specific service continuity plans. *(The development and management of service continuity plans are addressed in the Service Continuity process area.)*

Typical work products

1. Results of business impact analysis (documenting public service dependencies for facilities)
2. List of public service providers on which facilities are dependent
3. Key contacts list
4. Updated service continuity plans

Subpractices

1. Identify and document public services on which facilities rely.

   Typically, this activity results from business impact analysis. However, it can be included as part of service continuity planning or facility asset definition, depending on the organization. A resulting list of public services for each facility should be documented and made available for inclusion in service continuity plans as appropriate.

2. Develop a key contacts list for organizational services that can be included as part of service continuity plans.

EC:SG4.SP4 Manage Dependencies on Public Infrastructure

Dependencies on public infrastructure for facility assets are identified and managed.

Facility assets are a primary point where an organization intersects physically with its geographical environment. Facilities are vitally dependent on public infrastructure and services to operate and to remain viable. These services include

- telecommunications and telephone services
- electricity, natural gas, and other energy sources
- water and sewer services
- trash collection and disposal, and other support services

These dependencies must be carefully evaluated for several reasons. First, the organization must be prepared to address the loss of these services, which can affect organizational services that are supported by a facility. Second, the organization may need to consider the resilience of public services when developing service continuity plans for a facility—the inability to retain telecommunications, power, or water services may adversely impact the organization's ability to execute the facility's service continuity plan. Consideration of these public services may also cause the organization to make decisions about capital improvements (such as implementing backup power systems) that would be necessary to ensure a minimal level of operational resilience for the facility.

Typical work products

1. Results of business impact analysis (documenting public infrastructure dependencies for facilities)
2. List of public infrastructure providers on which facilities are dependent
3. Key contacts list
4. Updated service continuity plans

Subpractices

1. Identify and document internal infrastructure dependencies that the organization relies upon to provide services.

   Remember that these dependencies may be internal as well as external, particularly when the organization has control over certain aspects of facility infrastructure such as power or telecommunications that it provides for its own operations.

   Typically, this activity results from business impact analysis. However, it can be included as part of service continuity planning or facility asset definition, depending on the organization. A resulting list of public infrastructure providers for each facility should be documented and made available for inclusion in service continuity plans as appropriate.

2. Identify and document external resources that the organization relies upon to provide services.

3. Develop a key contacts list for public infrastructure services that can be included as part of the service continuity plans.
4. Update service continuity plans as appropriate.

   This practice may result in updates to existing service continuity plans or in the development of actions and activities that seek to provide an acceptable minimum level of redundancy in certain public infrastructure services.

EC:SG4.SP5 Plan for Facility Retirement

Facility retirements are planned in order to minimize operational impact.

The retirement of a facility can have widespread and unintended effects on the resilience of organizational services. If it is not appropriately planned and executed, temporary or permanent disruptions in operations can result. This is particularly true for facilities because they serve as a convergence point for many organizational services. Thus, the organization must carefully plan and execute the retirement of a facility (and the cut-over to a new facility, if planned) so that disruption can be minimized and any potential impacts can be identified in advance and appropriately addressed. In some cases, this may require the organization to develop special-purpose service continuity plans (or enhance existing plans) to address the unique issues that may result from retirement.

Typical work products

1. Facility retirement standards and guidelines
2. Service continuity plans (specific to retirement)
3. List of business partners and vendors that facilitate service delivery and will be affected by facility retirement
4. Key contacts list

Subpractices

1. Develop a plan for facility retirement.

   This practice applies not only to facilities that the organization owns but also to the retirement of a service contract for an outside facility that the organization leases or shares with another organization.

   As part of the plan, the organization should identify and document the services that will be affected by the facility retirement and include the stakeholders of these services in the planning process.

2. Develop and implement service continuity plans to support the retirement of the facility asset.

   These plans are developed to ensure that potential problems that arise in the retirement of the facility do not affect the operational resilience of services that rely on the facility. These plans may be temporary or sufficiently generic that they can be used whenever facilities are retired.

3. Archive facility work products.

This may include any facility training manuals, service continuity plans, maintenance records, and other documents that may have to be referenced by the organization in the future.

4. Retire the facility by executing the retirement plan.

   This includes monitoring the retirement for any potential problems and executing service continuity plans where necessary.

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 Environmental Control process area.

EC:GG1 Achieve Specific Goals

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

EC:GG1.GP1 Perform Specific Practices

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

Elaboration:

Specific practices EC:SG1.SP1 through EC:SG4.SP5 are performed to achieve the goals of the environmental control process.

EC:GG2 Institutionalize a Managed Process

Environmental control is institutionalized as a managed process.

EC:GG2.GP1 Establish Process Governance

Establish and maintain governance over the planning and performance of the environmental control process.

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

Subpractices

1. Establish governance over process activities.

   Elaboration:

   Governance over the environmental control process may be exhibited by

   - establishing a higher level management position responsible for the resilience of the organization's facility assets
   - developing and publicizing higher level managers' objectives and requirements for the process

- providing oversight over the development, acquisition, implementation, and management of high-value facility assets
- sponsoring process policies, procedures, standards, and guidelines, including the documentation of facility assets and establishing asset ownership and custodianship
- providing oversight over the establishment, implementation, and maintenance of the organization's internal control system for facility assets
- making higher level managers aware of applicable compliance obligations related to environmental control, and regularly reporting on the organization's satisfaction of these obligations to higher level managers
- sponsoring and funding process activities
- providing guidance for prioritizing facility assets relative to the organization's high-priority strategic objectives
- providing guidance on identifying, assessing, and managing operational risks related to facilities, including guidance for ensuring facility asset availability during disruptive events
- regular reporting from facility asset owners to higher level managers on facility controls and 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 audit committees on facilities 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 environmental control policy should address

- responsibility, authority, and ownership for performing process activities, including establishing and implementing administrative, technical, and physical controls to meet resilience requirements
- access to facilities, such as who can enter, when, and under what conditions or criteria
- clean desk and clean screen policies
- procedures, standards, and guidelines for
  - facility site selection, construction, and management (addressing issues of co-location, geographical dispersion, proximity, etc.)
  - facility retirement
  - documenting facility asset descriptions and relevant information
  - describing facility owners and custodians
  - managing dependencies on public services and public infrastructure, including establishing agreements or credentialing with public-private service providers
  - developing and documenting resilience requirements for facility assets
  - establishing, implementing, and maintaining an internal control system for facilities *(Refer to EC:SG2.SP2.)*
  - maintaining environmental conditions for facilities

  - managing facility operational risk
  - establishing facility service continuity plans and procedures
  - retiring facilities at the end of their useful life
  - health and safety
  - evacuation
  - fire suppression and handling
  - disruptive event handling such as hardware failure, bomb threats, and loss of electrical power, water, or other utilities
- the association of facility assets to core organizational services, and the prioritization of assets for service continuity
- methods for measuring adherence to policy, exceptions granted, and policy violations

EC:GG2.GP2 Plan the Process

Establish and maintain the plan for performing the environmental control process.

Elaboration:

The plan for performing the environmental control process is created to ensure that facility assets remain available and viable to support organizational services. The plan must address the resilience requirements of the facility assets, dependencies of services on these facility assets, and consideration of multiple asset owners and custodians at various levels of the organization. In addition, because facilities have a strong geographical connection, the plan must extend to external stakeholders that can enable or adversely affect facility resilience.

Subpractices

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

   Elaboration:

   Special consideration in the plan may have to be given to the establishment, implementation, and maintenance of an internal control system for facility assets, as well as facility sustainability planning. These activities address the protection and sustainability of the facility asset commensurate with its 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.

EC:GG2.GP3 Provide Resources

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

Elaboration:

The diversity of activities required to protect and sustain all types of facility assets requires an extensive level of organizational resources and skills and a significant number of external resources (for example, as described in EC:SG4.SP3 for public services and in

EC:SG4:SP4 for public infrastructure). 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 environmental control process:

   - staff responsible for
     - identifying high-value facility assets and the services with which they are associated
     - establishing and maintaining physical security (such as security guards)
     - managing changes to facility asset requirements, controls, strategies, and plans (This includes communicating changes to affected stakeholders, including asset owners and custodians.)
     - developing process plans and supporting the development of facility service continuity plans and ensuring they are aligned with stakeholder requirements and needs
     - managing external entities that have contractual obligations for managing facility assets
   - information, application, and technical security staff
   - business continuity and disaster recovery staff
   - IT operations and service delivery staff
   - facilities management staff
   - technicians who implement and maintain physical security access and surveillance systems
   - staff involved in facilities risk management, including insurance and risk indemnification staff
   - staff involved in maintaining the physical plant (such as HVAC contractors)
   - staff involved in providing public services and public infrastructure to facilities
   - contractors responsible for the construction of facilities
   - owners and custodians of facility 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.

   Elaboration:

   At a minimum, funding must be available to support the establishment, implementation, and maintenance of an internal control system for facilities, as well as the development, implementation, testing, and execution of service continuity plans for

facilities. In some cases, capital funding may be required for projects that enhance or support the protection and sustainability of facilities, which may result in developing additional facilities or establishing contracts with external entities to provide or support facilities when needed.

Refer to the Financial Resource Management process area for information about budgeting for, funding, and accounting for environmental control. Refer to the External Dependencies Management process area for information about establishing and managing relationships with external entities.

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

Elaboration:

Because of the extensive level of controls that have to be implemented and managed, necessary tools, techniques, and methods will be diverse. An example of a necessary tool for managing the environmental control process for facilities is a physical access system (such as a card reader, biometric device, or proximity reader).

In addition, developing and maintaining the facility inventory may require tools, techniques, and methods that allow for asset documentation and profiling, reporting, and updating on a regular basis. The need for these tools may be greater if the asset inventory is developed across many organizational units and must be aggregated at the enterprise level. The facility asset inventory database should be searchable and expandable to include additional information such as documentation of associated services and the asset's resilience requirements.

These are examples of tools, techniques, and methods for managing facility assets:

- methods for identifying and prioritizing high-value assets
- techniques and tools for documenting and profiling assets
- methods and techniques for assigning resilience requirements to facility assets and determining the extent to which facility assets satisfy these requirements
- methods, techniques, and tools for controlling physical access to facility assets, such as controlled entry gates, lighting, fencing, motion detectors, picture IDs, locks, and card readers
- logging, monitoring, and auditing tools to detect and report unauthorized access and use of facilities *(Refer to the Monitoring process area.)*
- environmental monitoring and control systems
- facility inventory tracking and monitoring systems (via RFID or other technology)
- systems for monitoring the viability of public services, such as electricity, gas, water, and telecommunications
- direct connection alarm systems that report to public authorities
- methods, techniques, and tools for identifying, assessing, and addressing risks to facility assets *(Refer also to the Risk Management process area.)*
- tools for managing the maintenance of environmental conditions, such as equipment service intervals, staff authorized to carry out repairs and service, suspected and actual faults, and maintenance change requests
- tools for managing public service and infrastructure provider and key contacts lists
- methods and tools for aggregating local asset inventories into an enterprise inventory

- asset inventory database management system
- methods, techniques, and tools for asset change management and control

EC:GG2.GP4 Assign Responsibility

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

Elaboration:

Of paramount importance in assigning responsibility for the environmental control process is the establishment of facility owners and custodians, which is described in ADM:SG1.SP3. Owners are responsible for establishing facility 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 facility 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 facility assets.

Subpractices

1. Assign responsibility and authority for performing the process.

   Elaboration:

   Responsibility and authority may extend to not only staff inside the organization but to those with whom the organization has a contractual (custodial) agreement for managing facilities (including implementation and management of controls and facility sustainability).

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

   Elaboration:

   Responsibility and authority for performing environmental control 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 facility assets under their ownership or custodianship
   - developing and implementing contractual instruments (including service level agreements) with external entities to establish responsibility and authority for performing process tasks on outsourced functions
   - including process activities 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 contractual instruments

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

EC:GG2.GP5 Train People

Train the people performing or supporting the environmental control process as needed.

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

Refer to the Human Resource Management process area for more information about creating an inventory of 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 environmental control process:

   - knowledge necessary to establish, implement, and maintain an internal control system for facilities as described in EC:SG2.SP2
   - ability to implement and manage physical constructs and systems for facilities such as HVAC systems, fire suppression, and utilities
   - knowledge necessary to identify, assess, and address facility operational risk to ensure risk is minimized to an acceptable level *(Refer to the Risk Management process area.)*
   - knowledge of the tools, techniques, and methods necessary to manage facility assets, including those necessary to perform the process using the selected methods, techniques, and tools identified in EC:GG2.GP3 subpractice 3
   - knowledge necessary to work effectively with asset owners and custodians and public service and public infrastructure providers, including strong communication skills
   - knowledge necessary to elicit and prioritize stakeholder requirements and needs and interpret them to develop effective process requirements and plans

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

3. Identify training opportunities to address skill gaps.

   Elaboration:

   Training may be particularly useful and necessary for asset owners who may not have the requisite skills for ensuring the protection and sustainability of facilities. Training may also be necessary for practitioners (such as security practitioners and maintenance contractors) who do not have specific experience in managing controls for facilities or in ensuring their sustainability.

These are examples of training topics:

- ensuring the protection and sustainability of facilities, particularly for asset owners and custodians
- for security practitioners and maintenance contractors, specific training in managing controls for facilities to ensure their sustainability, particularly when dealing with a disruptive event
- dealing effectively with public service and public infrastructure providers
- supporting 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 EC:GG2:GP3 subpractice 3

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

EC:GG2.GP6 Control Work Products

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

Elaboration:

All work products related to facility administrative, technical, and physical controls (such as configurations, logs, policies, standards, records, etc.) should be placed under control.

In addition to the specific work products included throughout the environmental control process, additional work products such as facility control documentation, control logs and exception reports (including physical security system logs), fire inspection reports, surveillance tapes or recordings, facility visitor logs, and facility asset retirement records may be placed under control.

These are examples of environmental control work products placed under control:

- facility asset inventory
- facility asset resilience requirements
- facility asset controls (administrative, technical, physical, and those with respect to design, leasing, co-location, and construction) and supporting documentation
- facility asset owners and custodians
- facility asset risk statements (categorized, prioritized, with impact valuation) and response plans
- service continuity plans that address facility sustainability
- facility equipment service levels, specifications, and authorized maintenance staff
- maintenance records, including change requests
- key contacts lists for public service and public infrastructure providers
- facility dependencies on public services and public infrastructure
- facility retirement standards, practices, and records
- process plan
- policies and procedures
- contracts with external entities

EC:GG2.GP7 Identify and Involve Relevant Stakeholders

Identify and involve the relevant stakeholders of the environmental control process as planned.

Elaboration:

The primary stakeholders for the environmental control process are facility asset owners and custodians. In addition, EC:SG4.SP5 calls for involving stakeholders in planning for facility retirement.

Subpractices

1. Identify process stakeholders and their appropriate involvement.

   Elaboration:

   Because of the significant connection between facilities and their geographic environment, a substantial number of stakeholders are likely to be external to the organization.

   These are examples of stakeholders of the environmental control process:

   - owners and custodians of facility assets, including external entities responsible for managing facility assets
   - staff responsible for managing operational risks to facilities
   - staff responsible for the physical security of facility assets
   - staff responsible for establishing, implementing, and maintaining an internal control system for facilities
   - staff required to develop, test, implement, and execute service continuity plans for facilities
   - staff involved in the retirement of facilities, including all affected service providers
   - 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
   - staff in other organizational support functions, such as accounting and general services administration (particularly as related to facility inventory valuation and retirement)

   Stakeholders are involved in various tasks in the environmental control process, such as

   - planning for the process, including facility retirement
   - creating a facility asset baseline
   - creating facility profiles
   - associating facility assets with services and analyzing asset-service dependencies
   - assigning resilience requirements to facilities
   - establishing, implementing, and managing facility controls
   - developing service continuity plans
   - managing facility risks
   - controlling facility operational environments
   - maintaining facilities and facility equipment
   - managing facility external dependencies

- 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.

EC:GG2.GP8 Measure and Control the Process

Measure and control the environmental control 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.

These are examples of metrics for the environmental control process:

- percentage of organizational facility assets that have been inventoried
- percentage of facility assets with/without a complete asset profile (such as no stated resilience requirements)
- percentage of facility assets with/without a designated owner
- percentage of facility assets with/without a designated custodian (if applicable)
- percentage of facility assets that have designated owners but no custodians (if applicable)
- percentage of facility assets that have designated custodians but no owners
- percentage of facility assets that have been inventoried, by service (if applicable)
- percentage of facility assets that are not associated with one or more services (if applicable)
- elapsed time since the facility asset inventory was reviewed
- percentage of facility asset-service dependency conflicts with unimplemented or incomplete mitigation plans
- percentage of facility asset-service dependency conflicts with no mitigation plans
- number of discrepancies between the current inventory and the previous inventory
- number of changes made to asset profiles in the facility asset inventory
- number of changes to resilience requirements as a result of facility asset changes
- number of changes to service continuity plans as a result of facility asset changes

- percentage of facility assets that are designated as high-value assets
- elapsed time since review and validation of high-value facility assets and their priorities
- percentage of facility assets that are resilience-focused (those required for service continuity & service restoration)
- elapsed time since review and reconciliation of resilience-focused facility assets
- percentage of facility assets without assigned/defined resilience requirements
- percentage of facility assets with assigned/defined resilience requirements that are undocumented
- percentage of facility assets that do not satisfy their resilience requirements
- percentage of facility assets with no or missing protection controls
- percentage of facility assets with no or missing sustainment controls (including controls over design, construction, and leasing)
- percentage of facility 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 facility 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 facility asset controls
- elapsed time since risk assessment of facility assets performed
- percentage of facility assets for which business impact valuation (qualitative or quantitative) has not been performed
- percentage of facility assets for which a risk assessment has not been performed and documented (per policy or other guidelines) and according to plan
- percentage of facility asset risks that have not been assigned to a responsible party for action, tracking, and closure
- percentage of facility asset risks with a disposition of “mitigate or control” that do not have a defined response plan
- percentage of facility asset risks with a “mitigate or control” disposition that are not effectively addressed by their response plans

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

Elaboration:

Periodic reviews of the environmental control process are needed to ensure that

- the facility asset inventory is accurate and complete
- newly acquired facility assets are included in the inventory
- changes to facility assets (additions, maintenance actions, retirements) are accurately reflected in the inventory
- the facility asset-service mapping is accurate and current
- ownership and custodianship over facility assets are established and documented
- access to the facility asset inventory is being limited to only authorized staff

- access to facility assets is limited to authorized staff
- status reports are provided to appropriate stakeholders in a timely manner
- facility asset-service dependency 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
- administrative, technical, and physical controls are operating as intended
- controls are meeting the stated intent of the resilience requirements
- actions resulting from internal and external audits are being closed in a timely manner

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

   Elaboration:

   Discrepancies result when facility assets are acquired, modified, or retired but not reflected accurately in the facility asset inventory. Assets form the foundation for operational resilience management because they are the target of strategies to protect and sustain them. To the extent that the environmental control process results in inventory discrepancies, the organization's overall ability to manage operational resilience is impeded.

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

   Elaboration:

   For facility 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.

EC:GG2.GP9 Objectively Evaluate Adherence

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

Elaboration:

These are examples of activities to be reviewed:

- identifying and prioritizing facility assets
- identifying facility resilience requirements
- establishing and implementing facility controls
- identifying and managing facility risks
- developing service continuity plans for facilities

- maintaining facility environmental conditions
- identifying and managing facility dependencies
- retiring facilities
- the alignment of stakeholder requirements with process plans
- assignment of responsibility, accountability, and authority for process activities
- determination of the adequacy of process reports and reviews in informing decision makers regarding the performance of operational resilience management activities and the need to take corrective action, if any
- verification of internal controls
- use of process work products for improving strategies for protecting and sustaining assets and services

These are examples of work products to be reviewed:

- facility asset inventory
- facility internal controls documentation
- facility risk statements
- facility risk response plans
- service continuity plans
- facility maintenance records and change logs
- business impact analysis results
- key provider and contact lists
- facility retirement standards
- process plan and policies
- dependency issues that have been referred to the risk management process
- process methods, techniques, and tools
- metrics for the process *(Refer to EC:GG2.GP8 subpractice 2.)*
- contracts with external entities

EC:GG2.GP10 Review Status with Higher Level Managers

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

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

EC:GG3 Institutionalize a Defined Process

Environmental control is institutionalized as a defined process.

EC:GG3.GP1 Establish a Defined Process

Establish and maintain the description of a defined environmental control process.

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

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

Subpractices

1. Select from the organization's set of standard processes those processes that cover the environmental control 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.

EC:GG3.GP2 Collect Improvement Information

Collect environmental control 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:

- facility asset inventory
- inventory inconsistencies and issues
- reports on the effectiveness and weaknesses of controls
- improvements based on risk identification and mitigation
- effectiveness of service continuity plans in execution
- lessons learned in post-event review of incidents and disruptions in facility continuity
- maintenance issues and concerns for facility infrastructure and physical plant
- conflicts and risks arising from dependencies on external entities
- lessons learned in retiring facilities from active use
- metrics and measurements of the viability of the process *(Refer to EC:GG2.GP8 subpractice 2.)*
- changes and trends in operating conditions, risk conditions, and the risk environment that affect process results
- lessons learned about the process that can be applied to improve operational resilience management performance, such as poorly documented or profiled assets and difficulties in assigning and executing asset ownership and custodianship responsibilities
- the level to which the facility asset inventory, asset profiles, and the asset database reflect the current status of all assets

- asset-service dependency response plans that are not executed and the risks associated with them
- resilience requirements that are not being satisfied or are being exceeded

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

Subpractices

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