

CERT[®] Resilience Management Model, Version 1.2

Service Continuity (SC)

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/>



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.

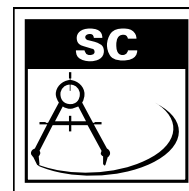
* These restrictions do not apply to U.S. government entities.

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

DM-0003234

SERVICE CONTINUITY

Engineering



Purpose

The purpose of Service Continuity is to ensure the continuity of essential operations of services and their associated assets if a disruption occurs as a result of an incident, disaster, or other disruptive event.

Introductory Notes

The continuity of an organization's service delivery is a paramount concern in the organization's operational resilience activities. The organization can invest considerable time and resources in attempting to prevent a range of potential disruptive events, but no organization can mitigate all risk. As a result, the organization must be prepared to deal with the consequences of a disruption to its operations at any time. Significant disruption can result in dire circumstances for the organization, even bankruptcy or termination.

Service Continuity describes the organizational processes responsible for developing, deploying, exercising, implementing, and managing plans for responding to and recovering from events and restoring operations to business as usual. This requires that the organization have a plan and program for service continuity, assign adequate and sufficient resources to the plan and program, and have the requisite infrastructure to carry out the plan and program. Based on risk appetite and tolerance, the organization must determine which service continuity plans it needs to establish, develop the plans, and exercise them on a regular and sufficient basis to ensure they remain viable as long as the service is vital to the organization.

The organization also must consider the range of service continuity activities. Business continuity or contingency plans are developed and implemented to sustain a high-value service, while recovery and restoration plans are focused on bringing services back to an acceptable level of business as usual. To ensure that all plans can be executed at will when called upon, the organization must also develop sufficient logistics and delivery capabilities.

Before the organization can develop, exercise, and position service continuity plans for implementation, several other organizational activities must occur. These include identification of

- the high-value services and associated assets for which service continuity plans must be developed (*This is addressed in the Enterprise Focus and Asset Definition and Management process areas.*)
- the potential hazards or risks to these high-value services and assets (*This is addressed in the Vulnerability Analysis and Resolution and Risk Management process areas.*)
- the consequences of these risks to the organization and its susceptibility to them (*This is addressed in the Risk Management process area.*)

In managing operational risk and resilience, the Service Continuity process area is complementary to Controls Management. Controls Management focuses on "condition

management” to prevent risk, while Service Continuity directs the organization’s attention to “consequence management” or planning for managing the consequences of risks that are realized. Together, these process areas provide a comprehensive, coordinated, optimized, and holistic approach to managing asset and service resilience.

Related Process Areas

The development, implementation, and management of an internal control system to prevent risks and disruptive events are addressed in the Controls Management process area.

The identification and management of incidents that may require the execution of a service continuity plan are addressed in the Incident Management and Control process area.

Providing training for staff involved in service continuity plan testing and execution is addressed in the Organizational Training and Awareness process area.

The identification and prioritization of the organization’s high-value services as strategic planning activities are addressed in the Enterprise Focus process area.

The consideration of consequences as a foundational element for developing a service continuity plan is addressed in the Risk Management process area.

The association of assets to the high-value services they support is performed in the Asset Definition and Management process area.

The development, implementation, and management of strategies for technology asset availability and integrity are addressed in the Technology Management process area.

The identification of vital records and databases for service continuity is addressed in the Knowledge and Information Management process area.

The resilience considerations of the organization’s reliance on public services and public infrastructure are addressed in the Environmental Control process area.

Summary of Specific Goals and Practices

Goals	Practices
SC:SG1 Prepare for Service Continuity	SC:SG1.SP1 Plan for Service Continuity
	SC:SG1.SP2 Establish Standards and Guidelines for Service Continuity
SC:SG2 Identify and Prioritize High-Value Services	SC:SG2.SP1 Identify the Organization's High-Value Services
	SC:SG2.SP2 Identify Internal and External Dependencies and Interdependencies
	SC:SG2.SP3 Identify Vital Organizational Records and Databases
SC:SG3 Develop Service Continuity Plans	SC:SG3.SP1 Identify Plans to Be Developed
	SC:SG3.SP2 Develop and Document Service Continuity Plans
	SC:SG3.SP3 Assign Staff to Service Continuity Plans
	SC:SG3.SP4 Store and Secure Service Continuity Plans
	SC:SG3.SP5 Develop Service Continuity Plan Training
SC:SG4 Validate Service Continuity Plans	SC:SG4.SP1 Validate Plans to Requirements and Standards
	SC:SG4.SP2 Identify and Resolve Plan Conflicts
SC:SG5 Exercise Service Continuity Plans	SC:SG5.SP1 Develop Testing Program and Standards
	SC:SG5.SP2 Develop and Document Test Plans
	SC:SG5.SP3 Exercise Plans
	SC:SG5.SP4 Evaluate Plan Test Results
SC:SG6 Execute Service Continuity Plans	SC:SG6.SP1 Execute Plans
	SC:SG6.SP2 Measure the Effectiveness of the Plans in Operation
SC:SG7 Maintain Service Continuity Plans	SC:SG7.SP1 Establish Change Criteria
	SC:SG7.SP2 Maintain Changes to Plans

Specific Practices by Goal

SC:SG1 Prepare for Service Continuity

The organizational processes for sustainability planning and execution are established.

Service continuity management requires both planning and execution. Planning involves establishing how the organization is going to address service continuity so that it is a consistent and pervasive organizational competency focused on operational resilience management. This involves developing a service continuity plan, establishing a service continuity program, assigning resources, and establishing service continuity standards and guidelines to ensure consistency.

SC:SG1.SP1 Plan for Service Continuity

Planning is performed for developing and implementing the organization's service continuity process.

Service continuity management is a fundamental organizational process that ensures that high-value organizational services—both internally and externally focused—are able to continue to achieve their missions when disruptions occur. Service continuity cannot be effectively managed by reaction—the organization must plan its approach to service continuity, align this plan with strategic objectives, provide sponsorship and oversight to the plan to ensure that it is accepted by the organization as a strategic function, and obtain organizational commitments to the plan to ensure that

service stakeholders understand and accept their responsibilities for service continuity.

The organization should develop and document its plan for service continuity and outline the specific objectives of the plan. The plan should reflect the organization's philosophy on service continuity and be translatable into a program for service continuity that can be implemented and managed.

The development of a plan for service continuity should not be confused with the development of service continuity plans. Service continuity plans are service-specific plans for sustaining services and associated assets under degraded conditions. A plan for service continuity is an organizational construct from which a service continuity program is developed and implemented as part of an operational resilience management system.

Typical work products

1. Plan for managing service continuity
2. Documented requests for commitment to the plan
3. Documented commitments to the plan

Subpractices

1. Establish the plan for managing service continuity.

The plan for managing service continuity should address at a minimum

- the organization's philosophy on service continuity
- the structure of the service continuity program and process
- the requirements of the service continuity program relative to managing operational resilience
- the means and activities involved in identifying and prioritizing services and assets for continuity
- the roles and responsibilities necessary to carry out the plan and the program
- applicable training needs and requirements
- resources that will be required to meet the objectives of the plan
- relevant costs and budgets associated with service continuity

2. Establish commitments to the plan.

Documented commitments by those responsible for implementing and supporting the plan are essential for plan effectiveness.

3. Revise the plan and commitments as necessary.

SC:SG1.SP2 Establish Standards and Guidelines for Service Continuity

The guidelines and standards for service continuity are established and communicated.

Guidelines and standards for service continuity ensure consistent plan documentation, distribution, testing, and execution enterprise-wide. They ensure that common, important elements of service continuity are considered by all organizational units and provide standards for consistent

documentation, testing, and handling of plans. Guidelines and standards also provide the organization an ability to view service continuity at an enterprise level and to manage this function to meet organizational goals.

Typical work products

1. Service continuity management guidelines and standards

Subpractices

1. Develop and communicate service continuity guidelines and standards.

Guidelines and standards are organization-specific but may address areas such as the following:

- plan ownership and responsibility
- requirements for when a plan must be developed
- documentation requirements for plans
- the standard content of plans (i.e., what must be addressed at a minimum)
- testing requirements for plans, including testing intervals and reporting of results
- identification and involvement of stakeholders
- plan distribution and communication
- plan versioning, storage, archiving, and security
- training standards for service continuity and plan execution

SC:SG2 Identify and Prioritize High-Value Services

The services that are required to meet the organization's mission are identified and prioritized.

The high-value services of the organization must be identified as a baseline for identifying the extent and types of service continuity plans to be developed and implemented. Failure to identify and prioritize these services may result in the development of service continuity plans that are unnecessary or ineffective and increases the operational resilience management costs for the organization.

Prior to building service continuity plans, the organization must prioritize services, analyze service dependencies and interdependencies, and identify associated information and knowledge that must be addressed in the plans.

SC:SG2.SP1 Identify the Organization's High-Value Services

The high-value services of the organization and their associated assets are identified.

The identification and prioritization of the organization's high-value services as strategic planning activities are addressed in the Enterprise Focus process area. This practice is included here to emphasize the importance of prioritizing high-value services as a foundational activity in the identification and development of service continuity plans.

A fundamental risk management principle is to focus on activities to protect and sustain services and assets that most directly affect the organization's ability to achieve its mission. Identifying high-value services, their associated assets, and the activities that support these services must be

performed before the organization attempts to develop service continuity plans.

The association of assets to the high-value services they support is performed in the Asset Definition and Management process area.

Typical work products

1. Prioritized list of high-value organizational services, activities, and associated assets
2. Results of security risk assessment and business impact analyses

Subpractices

1. Identify the organization's high-value services, associated assets, and activities.
2. Analyze and document the relative value of providing these services and the resulting impact on the organization if these services are interrupted.

Consideration of the consequences of the loss of high-value organizational services is typically performed as part of a business impact analysis. In addition, the consequences of risks to high-value services are identified and analyzed in risk assessment activities. The organization must consider this information when prioritizing high-value services.

The consideration of consequences as the result of risk is addressed in the Risk Management process area.

3. Prioritize and document the list of high-value services that must be provided if a disruption occurs.

The identification and prioritization of the organization's high-value services as strategic planning activities are addressed in the Enterprise Focus process area.

SC:SG2.SP2 Identify Internal and External Dependencies and Interdependencies

The internal and external relationships necessary to ensure service continuity are identified and analyzed.

The resilience considerations of the organization's reliance on public services and public infrastructure are addressed in the Environmental Control process area. The association of internal and external assets to the services they support is addressed in the Asset Definition and Management process area. Managing relationships with external entities is addressed in the External Dependencies Management process area. This practice is included here to emphasize the need to determine the layers of support on which services depend in order to develop effective and comprehensive service continuity plans.

Services depend on organizational assets, both internal and external, to ensure continuity of operations. They also rely on external entities such as public agencies and infrastructure such as public utilities and telecommunications. These dependencies and interdependencies must be

identified in order to ensure a robust consideration of the range of planning that must be incorporated into the service continuity plans.

Typical work products

1. List of public service providers on which services depend (*Refer also to EC:SG4.SP3 and SP4.*)
2. List of external entities, including business partners and vendors that facilitate service delivery
3. Key contacts list

Subpractices

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

This practice requires that the organization document the association between services and the internal and external assets—people, information, technology, and facilities—that support the services. (This practice is formally performed in the Asset Definition and Management process area.)

2. Identify and document external entities that the organization relies upon to provide services.
3. Develop a key contacts list for organizational services that can be included as part of the service continuity plans.

SC:SG2.SP3 Identify Vital Organizational Records and Databases

Vital information required for service continuity is identified.

The resilience of information is addressed in the Knowledge and Information Management process area. This practice is included here to emphasize the importance of information assets in the development of effective and comprehensive service continuity plans.

Vital records and databases constitute high-value information assets that are essential to the continued operation of services during and after a disruption. Thus, these assets must be considered in the development of service continuity plans. Because information in the form of vital records and databases tends to be distributed organization-wide, vital records and databases must be inventoried to ensure that they are properly included in the service continuity plans. (*Developing and maintaining a comprehensive asset inventory are addressed in the Asset Definition and Management process area.*)

Vital records are typically distinguished from other types of information. Vital records include those records that the organization relies upon to protect the legal and financial rights of the organization and of individuals directly affected by disruption. In contrast, files and databases are types of information that are most typically associated with the direct operation of a specific service. For example, the vendor database is a necessary component of paying invoices. Vital records may be more universal in that they can apply to many service continuity plans, while files and databases may be more applicable to specific services.

Typical work products

1. Vital records, such as
 - organizational orders of succession
 - delegations of authority
 - contracts and service level agreements with external entities, including vendors and business partners
 - organizational legal operating charters
 - personnel records
2. Directory of vital staff (people assets) with contact information, roles, and responsibilities
3. List of files and databases that support high-value service operation

Subpractices

1. Identify and document vital records and databases.
This practice is formally performed in the Knowledge and Information Management process area.
2. Identify and document vital staff and their specific roles in relation to the services being provided.
This practice is formally performed in the People Management process area.
3. Ensure that vital records and databases are protected, accessible, and usable if a disruption occurs.
This practice is performed in the Knowledge and Information Management process area.

SC:SG3 Develop Service Continuity Plans

Service continuity plans for high-value organizational services are developed.

Service continuity plans are a proactively established description of the actions an organization will take if a service disruption occurs. They are generally focused on managing the organizational consequences of service disruption based on a range of potential events that can cause disruption, such as incidents and disasters. Service continuity plan development is in essence a risk management and control activity that seeks to limit or control the consequences of realized risk. Thus, the genesis for a service continuity plan may be risk assessment and mitigation activities or lessons learned from past disruptions.

Service continuity plans can take many forms, and often a service continuity plan is the aggregation of more than one type of plan.

These are examples of types of service continuity plans:

- Business continuity plans focus on the continued provision of a service under degraded circumstances.
- Recovery plans focus on limiting and containing damage as a result of the disruption and dealing with the consequences of the disruption.
- Restoration plans focus on performing the actions necessary to bring a service back to its expected and normal level of operation and output (as was in place before the disruption).

Typically, continuity and recovery plans provide for immediate, response-driven activities, while restoration plans are longer term activities that may extend for a considerable time after the immediate consequences of disruption have been experienced.

Service continuity plans are best developed when they are the result of a comprehensive and optimized consideration of the requirements for protecting and sustaining a service. In other words, as a foundation for operational resilience, the organization should develop service continuity plans as a part of implementing strategies for protecting and sustaining services and assets to meet resilience requirements.

Service continuity plans come at a cost to the organization. The development and maintenance of these plans are cost-intensive, as is the regular exercising of the plans to ensure they work as intended. Executing a service continuity plan is also costly to the organization. Thus, the cost of these plans must be evaluated and balanced with protective controls that have been implemented to prevent disruption and the value of the services and assets that would be disrupted.

The development of service continuity plans involves the identification of plans to be developed, the development of the plans, the assignment of resources to the plans, and the maintenance of the plans.

SC:SG3.SP1 Identify Plans to Be Developed

Required service continuity plans are identified.

The organization identifies the service continuity plans to be developed, tested, executed, and maintained. This can be done through several means:

- in the regular course of designing and implementing resilience requirements for services and assets
- as the result of security risk assessment and management activities (in the development of preventive controls and mitigation actions)
- as part of the business impact analysis process (a typically business-continuity-driven activity that seeks to identify the consequences of service disruption)
- as a result of legal, regulatory, compliance, and audit activities (where existing controls may not be deemed as effective across a range of potential disruptive events)
- in response to a major event or catastrophe (whether or not the organization was affected)

Typical work products

1. List of service continuity plans (to be developed)

Subpractices

1. Identify service continuity plans to be developed.

SC:SG3.SP2 Develop and Document Service Continuity Plans

The required service continuity plans are developed and documented.

Required service continuity plans are developed by the organization or its assigned representatives. Plans are typically developed by the service owner, but this varies by organization and might include significant involvement of IT staff if the service is highly automated or has one or more application systems associated with it.

The contents of the plan and the documentation requirements are established by the organization as part of the organization's service continuity standards and guidelines. This ensures consistency and enterprise-wide understandability and applicability.

The development of service continuity plans occurs as both a foundational and an ongoing activity. Plans are developed at the time of service development and implementation but also on an ongoing basis as new risks are encountered and the operational environment changes.

Typical work products

1. Service continuity plan templates
2. Service continuity plans (including relevant stakeholders)

Subpractices

1. Document the service continuity plans using available templates as appropriate.

A service continuity plan typically includes the following information:

- identification of authority for initiating and executing the plan (plan ownership)
 - identification of the communication mechanism to initiate execution of the plan
2. Document the key elements of the specific plan, including
 - alternative activities that would have to be performed (technical or manual)
 - alternative resources and locations that would support the organization's high-value services
 - identification of
 - vital staff roles and responsibilities
 - high-value technology assets necessary to support the plan
 - high-value information assets and vital records necessary to support the plan
 - high-value facilities assets necessary to support the plan
 - relevant stakeholders of the plan and method of communicating with them
(See subpractice 3 below.)
 - documentation of
 - the recovery sequence for the service
 - the restoration sequence for the service
 - applicable recovery time objectives and recovery point objectives (The establishment of RTOs and RPOs is addressed in the Technology Management process area.)

- security- and access-related issues that are required to execute the plan
- any special handling of information or technology that is required
- the test plan for the service continuity plan (See SC:SG5.SP2.)
- the service continuity training plan
- coordination activities with other internal staff and external entities that must be performed to implement the strategy
- the levels of authority and access needed by responders to carry out the strategy and plan
- the cost of the plan and the activities necessary to carry out the plan
- the logistics of the plan

Documentation of the plan must be consistent with the standards and guidelines established by the organization to ensure plan consistency, accuracy, and ability to implement. (See SC:SG1.SP2.)

Consider also that the service continuity plan may in reality require the development of one or more subplans (such as a restoration plan or a recovery plan).

3. Identify the stakeholders of specific service continuity plans.

Service continuity plans may have many different stakeholders. In addition to those who must execute and participate in the plans, other organizational groups (both internal and external) may have a vested interest in understanding them. For example, plans may be provided to public emergency management staff, to suppliers and vendors, and to external entities to which the organization is a supplier. These organizations may even have a stated role in the plans. In addition, some regulatory and legal entities may require that the organization submit service continuity plans as evidence that they have taken appropriate actions to prepare for specific threats such as natural disasters or terrorism.

Because there are many stakeholders for service continuity plans, the organization must identify the relevant stakeholders and communicate the plans to these stakeholders as necessary.

These are examples of relevant stakeholders:

- higher level managers
- service and asset owners
- vendors, suppliers, and business partners
- public entities such as emergency management, public utilities, public infrastructure, and local government
- regulatory and legal entities
- industry groups (for response coordination)

Communicate the service continuity plans to stakeholders and review and adjust them as necessary.

Ensure that compliance obligations that require communication and submission of service continuity plans are identified and satisfied. (*Meeting compliance obligations is addressed in the Compliance process area.*)

SC:SG3.SP3 Assign Staff to Service Continuity Plans

Staff members are assigned to the service continuity plans to ensure effective execution.

The activities documented in the service continuity plans must be assigned to responsible and skilled individuals in the event that the plans must be executed. These staff members may be internal to the organization or external (through outsourcing arrangements and service contracts). The organization must define the staff requirements that are required to meet the objectives of the plans, identify potential internal and external staff who will be needed to meet these requirements, and assign staff to activities in the plans.

When staff members do not have the necessary skill sets to meet the basic, minimum requirements of the plans, the organization must provide training and ascertain that the staff members are able to perform to the objectives stated in the plans as a result of this training. (*Training for service continuity plans is addressed in SC:SG3.SP5.*)

Typical work products

1. Service continuity plan staff requirements
2. List of potential staff members (to fulfill staff requirements)
3. Staff and task assignments (as documented in service continuity plans)
4. Staff commitments to service continuity plans

Subpractices

1. Identify staff requirements to satisfy the objectives of the service continuity plans.
2. Identify staff members, both internal and external, to satisfy the resource requirements.
3. Assign staff to the service continuity plans.

Ensure that those who are assigned tasks in the plans are aware of their assignments, have the authority to act as prescribed in the plans, and are held accountable for their activities. Ensure that these staff members commit to performing their roles as described in the plans.

SC:SG3.SP4 Store and Secure Service Continuity Plans

Service continuity plans are stored and made accessible to those with a need to know.

The ability to execute service continuity plans during a disruption is related to their accessibility and viability. When service continuity plans that are developed but misplaced or are allowed to be changed at will, they are not usable by those who are responsible for executing them. Given that many service continuity plans are executed under emergency or crisis circumstances, the ability to know where the current version of the plans is stored is invaluable. To achieve this, the organization must take steps to ensure that the plans are archived, that the most current versions of the

plans are available, that the plans are secured and free from intentional or unintentional modification, and that those who need to access the plans can readily retrieve them when necessary.

An inventory of service continuity plans can be established through the development and maintenance of a service continuity database. This allows the organization to secure access, provides a one-stop place to archive plans, and allows for plan version control. It also provides a means from which to perform plan maintenance and change control. (*Change control over service continuity plans is addressed in SC:SG7.*)

Typical work products

1. Service continuity plan inventory or database

Subpractices

1. Establish a service continuity plan inventory or database.
2. Store and protect the service continuity plans in the plan inventory or database.

Ensure that the service continuity plans are properly protected but accessible on demand to those who have proper authorization.

3. Establish access controls to ensure that service continuity plans can be accessed only by authorized individuals.

SC:SG3.SP5 Develop Service Continuity Plan Training

Training in the service continuity plans is developed and administered.

Training is an effective means for ensuring that participants in service continuity plans understand their roles and are capable of carrying out these roles in times of disruption and emergency. It is a means for communicating the contents of the service continuity plans to stakeholders and for ensuring that those responsible for carrying out the plans are qualified. Effective training increases the organization's capability in executing the plans and for ensuring that the plans' objectives are met. Poor advance training in service continuity plans often is a major contributor to their failure, which is typically learned under undesirable and unstable organizational conditions.

Not all staff members who are assigned to plans may have the requisite skills to perform the tasks they have been assigned. Thus, the organization must determine any skill gaps and ensure that appropriate training is made available and completed before the service continuity plans are validated.

The provision of training for skill sets necessary to execute service continuity plans is addressed in the Organizational Training and Awareness process area.

Typical work products

1. List of skill needs and gaps
2. Training strategy

3. Training records
4. Service continuity plan training materials
5. Training feedback evaluations

Subpractices

1. Identify any specialized training needs based on skill gaps for the activities described in the plans.

2. Develop a strategy for conducting service continuity plan training.

The strategy should address how the training is delivered and the means by which the competency of the resources involved is ascertained. The strategy should also note the frequency of training offerings and how participation in the training is documented.

3. Develop training materials and resources to conduct plan training on a regular and ongoing basis.
4. Train staff as necessary to fulfill their responsibilities in the plan.
5. Update service continuity plans, if necessary, as a result of feedback from training.

SC:SG4 Validate Service Continuity Plans

Service continuity plans are validated to ensure they satisfy standards and guidelines and to resolve conflicts between plans.

Before plans can be executed, the organization must validate the plans to ensure that they meet the organization's standards and guidelines, that they enable the satisfaction of resilience requirements, and that plans do not cause resource conflicts or other potential bottlenecks.

The identification, documentation, and analysis of operational resilience requirements for services and associated assets are addressed in the Resilience Requirements Development process area.

The management of requirements for services and associated assets is addressed in the Resilience Requirements Management process area.

SC:SG4.SP1 Validate Plans to Standards and Guidelines

Service continuity plans are examined to ensure they satisfy standards and guidelines.

The service continuity plans are part of the organization's overall operational resilience management strategy for services and assets. In essence, the plans are one of many functional controls that the organization implements to ensure that services and assets are resilient to disruption and interruption. Thus, service continuity plans are a means for satisfying the resilience requirements of services and assets. As a result, service continuity plans must be objectively reviewed to ensure that they are sufficient given the resilience requirements of related services and assets.

In addition, to ensure plan consistency, accuracy, completeness, and effectiveness, service continuity plans are examined against the

organization's standards and guidelines for plan development. This ensures consistent levels of documentation, the inclusion of required elements (such as stakeholders), and the ability of the plans to meet stated objectives. This also provides the organization an ability to review the logic of the plans and to make appropriate adjustments where inconsistencies or gaps are found.

Typical work products

1. Requirements gaps
2. Plan content issues and concerns
3. Plan updates and remediation actions

Subpractices

1. Review plans for consistency in achieving stated resilience requirements for services and associated assets.
2. Review plans for adherence to service continuity plan development standards and guidelines (*refer to SC:SG1.SP2*).
3. Identify plan omissions, gaps, and issues, and develop appropriate plan updates and remediation actions.

The plan walk-through can identify issues that pose risk to the organization because of poor coverage, inability of a plan's stated activities to meet objectives, poor documentation, etc. These issues must be identified and addressed as risks to meeting the related service or asset resilience requirements. As with all risks, proper risk disposition and mitigation actions should follow this practice.

Managing risks to high-value services and assets is addressed in the Risk Management process area.

SC:SG4.SP2 Identify and Resolve Plan Conflicts

Conflicts between service continuity plans are identified and resolved.

Because of the sheer volume of service continuity plans and the operational interconnection of many services and assets, service continuity plans often overlap or place reliance on the same set of organizational resources. For example, an organization may have an off-site facility that is named in more than one plan as a backup site, but if more than one plan is executed simultaneously, the facility may not be able to satisfy requirements as prescribed in any single plan. More commonly, some people are often named in multiple service continuity plans that may have to be executed simultaneously. These types of conflicts must be identified and resolved.

Typical work products

1. Plan conflicts
2. Plan updates and remediation actions

Subpractices

1. Review plans to determine plan conflicts.

2. Determine the severity of plan conflicts and develop appropriate mitigation actions to reduce or eliminate the conflicts.

Conflicts that would impede successful plan execution pose operational risks that must be mitigated by the organization. Remember that the conflict may affect more than one plan, and therefore mitigation actions may have to be performed on more than one plan.

These are examples of possible actions the organization can take to resolve conflicts:

- Revise or rewrite conflicting plans.
- Prioritize plans to make use of conflicting resources.
- Resolve conflicting resources by replacing them with other resources.
- Provide training for staff members who would be affected by plan conflicts.

3. Rewrite or revise plans as necessary.

SC:SG5 Exercise Service Continuity Plans

Service continuity plans are exercised to ensure they meet their stated objectives.

In addition to validation, service continuity plans must be tested (typically called “exercised”) on a regular basis to ensure that they will achieve their stated objectives when executed as the result of a disruption. Testing provides information about the effectiveness of the plan in advance of its use and provides an opportunity to improve the plan based on the test results.

To perform plan exercises, the organization must develop a testing program and standards (to ensure consistent test objectives and results), document test plans, test the plans, and debrief the test results to identify potential improvements and revisions.

SC:SG5.SP1 Develop Testing Program and Standards

A program and standards for service continuity plan testing are established and implemented.

Having a test program and standards helps ensure regular and consistent testing of service continuity plans to ensure their viability during an event or emergency. Testing is conducted in a controlled and measured environment and is the only opportunity for the organization to know whether the plans it has developed will achieve the stated objectives and satisfy requirements.

The organization establishes the plan testing standards, structure, and reporting requirements. The testing program and standards are enforced for all plan owners and developers to ensure consistency, comparability, and ability to interpret results at the organizational level. In addition, a consistent schedule of plan testing is established based on factors such as risk, potential consequences to the organization, and other organizationally derived factors. A quality review capability is established to review the results of plan tests and to look for trends and other information that could be used in improving the general state of service continuity plans and the testing of plans.

Typical work products

1. Plan test program
2. Plan test standards
3. Plan test schedule

Subpractices

1. Develop a testing program and test standards to apply universally across all testing of service continuity plans.

The test program and test standards should address the following, at a minimum:

- the organization’s strategy for conducting service continuity plan tests
- the establishment of high-quality test objectives
- the level of involvement and commitment of plan stakeholders in the testing of the plan
- reporting of test results
- quality assurance review of test results
- guidelines for addressing testing issues and concerns
- guidelines on frequency of testing

2. Establish schedules for ongoing testing and review of plans.

SC:SG5.SP2 Develop and Document Test Plans

Service continuity test plans are developed and documented.

Service continuity test plans must be documented to ensure that all involved in a test understand the test objectives, their roles in the test, and the manner in which the test will be conducted. Those with the most specific knowledge of the service continuity plan should be involved in developing and documenting the test plan.

One of the most important parts of the test documentation is the establishment of test objectives—what the test should be able to prove or disprove. Documenting a test plan also involves detailing specific information about the test environment and stakeholders involved in the test.

Typical work products

1. Service continuity plan test plans

Subpractices

1. Develop and document service continuity test plans.

The elements to be contained in a service continuity test plan include

- stakeholders involved in the testing exercise
- roles of each of the stakeholders and what is expected of them
- objectives of the test (such as testing RTOs and RPOs)
- specific test activities to be performed
- infrastructure requirements—information, technology, and facilities—and other conditions necessary to perform the test

- expected test results
- how to document and record the results of the test for later review

2. Review service continuity test plans with stakeholders.

SC:SG5.SP3 Exercise Plans

Service continuity plans are exercised on a regular basis and results are documented.

On a regular basis, service continuity plans are exercised (tested) according to their test plan. The test should establish the viability, accuracy, and completeness of the plan. It should also provide information about the organization's level of preparedness to address the specific area(s) included in the plan. The test is performed under conditions established by the organization and the results of the test are recorded and documented.

Typical work products

1. Documented results of plan testing

Subpractices

1. Prepare to conduct service continuity plan tests.

Ensure that all staff involved in the testing understand their roles, are equipped and trained to participate in the test, and understand how to document results. Ensure that testing infrastructure has been obtained and established, that other conditions have been met, and that all stakeholders have been notified of the test.

2. Execute the service continuity plan test.
3. Document and record the results in accordance with the organization's testing standards.

SC:SG5.SP4 Evaluate Plan Test Results

Opportunities for improving service continuity are identified and implemented as a result of exercising.

The objective for developing and executing service continuity plan tests is to ensure that the plans work as intended, but also to identify required improvements to the plans, the test plans, and possibly the plan for managing service continuity.

The evaluation of test results involves comparing the documented test results against the established test objectives. Areas where objectives could not be met are recorded and strategies are developed to review and revise the plans. Improvements to the testing process and plans are also identified, documented, and incorporated into future tests.

Typical work products

1. Documented results of test result analysis
2. Notable discrepancies between expected and actual test results
3. List of improvements to service continuity plans
4. List of improvements to service continuity test plans

5. List of improvements to the plan for managing service continuity

Subpractices

1. Compare actual test results with expected test results and test objectives.
2. Document areas of improvement for service continuity.

These are examples of improvement areas that may arise from plan testing:

- plan activities that do not achieve objectives as documented
- actual test results that do not match expected test results when expected test results are deemed valid
- shortcomings in test plans
- required changes to infrastructure
- plan logistics that may need revision
- lack of appropriate or sufficient resources
- training gaps for plan staff and stakeholders
- plan conflicts (particularly if more than one plan is tested simultaneously)
- actual costs of executing the plans versus expected costs

SC:SG6 Execute Service Continuity Plans

Service continuity plans are executed and reviewed.

Service continuity plans may be executed for a variety of reasons. Plans may be implemented in response to a perceived or known threat, as the result of an incident, or as a means to address an immediate crisis. Organizations may also implement their service continuity plans for other, less urgent reasons such as during the cut-over from one application system to another, while an office location is being moved, or as part of an organizational merger or acquisition.

Whatever the catalyst for executing the plan, the organization must be able to determine when the plan must be executed and who is responsible for initiating action.

Service continuity plans may be executed in response to an incident. (*The management of incidents and the organization's response is addressed in the Incident Management and Control process area.*)

SC:SG6.SP1 Execute Plans

Service continuity plans are executed as required.

The service continuity plans are executed as organizational conditions require.

Typical work products

1. Organizational conditions for executing service continuity plans
2. Documented results of executed service continuity plans

Subpractices

1. Determine the conditions under which a service continuity plan must be executed.

Ensure that the owners of service continuity plans understand these conditions and have the authority and responsibility to execute the plans if necessary.

2. Execute plans as required.

SC:SG6.SP2 Measure the Effectiveness of the Plans in Operation

Post-execution review is performed to identify corrective actions.

The debriefing of the execution of service continuity plans is an invaluable means for identifying plan shortcomings and for improving the plans. Plan improvements are documented through this process and incorporated into future plan versions. In some cases, new plans are developed in addition to or as replacements for existing plans. Logistical considerations of the plans are reviewed and analyzed, and changes are recommended. Unforeseen circumstances that arise during the execution of the plans—due to either the incident or the execution of the plan activities—are documented and addressed.

Typical work products

1. List of improvements to service continuity plans
2. List of improvements to service continuity test plans
3. List of improvements to the plan for managing service continuity

Subpractices

1. Compare documented service continuity plan results with plan objectives and expectations.
2. Document areas of improvement for service continuity.

Examples of areas of improvement that may result from plan execution are similar to those included in practice SC:SG5.SP4.

3. Document areas of improvement for testing service continuity plans.

SC:SG7 Maintain Service Continuity Plans

Changes to service continuity plans are identified and managed.

The testing and execution of service continuity plans are two sources of potential changes. However, the dynamic operating environment, sources of new threats and risks, and changes in other organizational entities such as staff, geographical locations, and relationships with external entities can require changes to service continuity plans and their corresponding test plans.

Because changes to plans may occur frequently, the organization must establish baseline criteria for changes and manage changes to the plans through regular review, updating, and version control.

SC:SG7.SP1 Establish Change Criteria

Change criteria for service continuity plans are established.

Because of changing operational and organizational conditions, service continuity plans may have a short useful life. Identifying and understanding

the types of organizational and operational triggers that may indicate a need to revisit and revise service continuity plans ensures that these plans remain viable.

Typical work products

1. Criteria for making changes to service continuity plans

Subpractices

1. Develop and document criteria for determining when changes to a service continuity plan should be considered.

These are examples of criteria (i.e., conditions) that may result in changes to service continuity plans:

- changes in a service's or asset's resilience requirements
- identification of new vulnerabilities, threats, and risks
- asset changes, such as staff changes, changes to information assets and technology, and relocation of facilities
- changes in a service's or asset's protective controls
- changes in the plan's stakeholders, including external entities and public agencies
- organizational changes, including staff and geographic changes
- changes in lines of business, industry, product or services mix
- significant technical infrastructure changes
- changes in relationships with external entities such as vendors and business partners
- changes in or additions to regulatory or legal obligations
- results of service continuity plan execution
- results of service continuity plan testing

SC:SG7.SP2 Maintain Changes to Plans

Changes are made to service continuity plans as conditions dictate.

Changes to service continuity plans are made as conditions dictate based on the change criteria established by the organization in practice SC:SG7.SP1. The changes are made to existing service continuity plans (although new plans may result), and versions of existing plans are incremented according to the organization's versioning protocol and standards.

Typical work products

1. Baseline service continuity plans (established upon initial plan development)
2. Updated service continuity plans (incremented version)
3. Updated service continuity plan inventory/database

Subpractices

1. Identify and document changes to service continuity plans based on defined criteria and conditions.

2. Increment versions of service continuity plans in the plan inventory/database.
3. Communicate the updated plans to appropriate stakeholders as required.

Elaborated Generic Practices by Goal

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

SC:GG1 Achieve Specific Goals

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

SC:GG1.GP1 Perform Specific Practices

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

Elaboration:

Specific practices SC:SG1.SP1 through SC:SG7.SP2 are performed to achieve the goals of the service continuity process.

SC:GG2 Institutionalize a Managed Process

Service continuity is institutionalized as a managed process.

SC:GG2.GP1 Establish Process Governance

Establish and maintain governance over the planning and performance of the service continuity process.

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

Subpractices

1. Establish governance over process activities.

Elaboration:

Governance over the service continuity process may be exhibited by

- sponsorship and oversight to ensure that the process is accepted by the organization as a strategic function with documented commitments to the plan and the process
- developing and publicizing higher level managers' objectives and requirements for the process
- sponsoring process policies, procedures, standards, and guidelines, including those for testing service continuity plans

- regular reporting from organizational units to higher level managers on service continuity process activities and results
- implementing a service continuity steering committee with oversight for all service continuity plans and test plans
- making higher level managers aware of applicable compliance obligations related to the process, and regularly reporting on the organization's satisfaction of these obligations to higher level managers
- sponsoring and funding process activities, including the development, documentation, and testing of service continuity plans
- aligning service continuity plans with identified resilience requirements and objectives and stakeholder needs and requirements, including the process plan
- 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
- creating dedicated higher level management feedback loops on decisions about the process and recommendations for improving the process
- providing input on identifying, assessing, and managing operational risks to services
- conducting regular internal and external audits and related reporting to audit committees on process effectiveness
- creating formal programs to measure the effectiveness of process activities, and reporting these measurements to higher level managers

2. Develop and publish organizational policy for the process.

Elaboration:

The service continuity policy should address

- responsibility, authority, and ownership for performing process activities
- procedures, standards, and guidelines for
 - plan ownership
 - plan documentation
 - plan content
 - testing of plans, including test objectives, reporting, and frequency
 - involvement of stakeholders
 - plan versioning, storage, archiving, and security
 - plan training
- responsibility and authority for developing, testing, and implementing service continuity plans
- communication of plans to stakeholders
- responsibility for testing (exercising) plans on a regular basis and methods used to do so
- making changes to plans
- post-plan reviews and revisions
- methods for measuring adherence to policy, exceptions granted, and policy violations

SC:GG2.GP2 Plan the Process

Establish and maintain the plan for performing the service continuity process.

Elaboration:

SC:SG1.SP1 requires the development of a plan for how the organization will carry out service continuity planning and execution. A plan for service continuity is an organizational construct from which a service continuity program is developed and implemented. In generic practice SC:GG2.GP2, the planning elements required in SC:SG1.SP1 and the plan for the service continuity process are formalized and structured and performed in a managed way. The plan for the service continuity process should be directly influenced by the strategic planning process of the organization and reflect strategic initiatives where appropriate.

The plan for the service continuity process should not be confused with a plan (and program) for service continuity or service-specific continuity plans (*refer to SC:SG3*). The plan for the service continuity process details how the organization will perform service continuity planning, including the development of service continuity plans. Service continuity plans are service-specific plans for sustaining services and associated assets under degraded conditions.

Subpractices

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

SC:GG2.GP3 Provide Resources

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

Elaboration:

SC:SG1.SP1 requires the assignment of resources to the plan for the service continuity process. SC:SG3.SP3 calls for the assignment of resources to service-specific continuity plans. In SC:GG2.GP3, resources are formally identified and assigned to process plan elements.

Subpractices

1. Staff the process.

These are examples of staff required to perform the service continuity process:

- staff responsible for
 - developing process standards and guidelines
 - developing service continuity plans, programs, and the process plan, and ensuring they are aligned with stakeholder requirements and needs
 - identifying high-value services and their associated assets
 - developing and maintaining the list of files and databases (vital records) that support high-value service operation

- the service continuity plan inventory/database
- developing and conducting service continuity training
- validating service continuity plans against requirements and standards
- service continuity plan testing
- identifying internal and external dependency relationships necessary to ensure service continuity
- managing changes to the plan for service continuity and service-specific continuity plans (This includes communicating changes to affected stakeholders, including service owners.)
- managing external entities that have contractual obligations for process activities
- service owners
- 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 service continuity.

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

Elaboration:

These are examples of tools, techniques, and methods to support the service continuity process:

- methods for identifying and prioritizing high-value services
- methods for analyzing service dependencies and interdependencies
- templates for developing and documenting service continuity plans
- methods, techniques, and tools for performing consistent and structured version control and for managing changes to service continuity plans
- tools for archiving, storing, and securing service continuity plans
- tools for providing access control over service continuity plan inquiries, modifications, and deletions
- tools for managing the service continuity plan inventory/database, including controlling access and managing changes
- methods for communicating with stakeholders (*Refer to the Communications process area.*)
- methods for distributing up-to-date versions of service continuity plans to stakeholders
- methods for analyzing plan dependencies and resolving conflicts
- methods, techniques, and tools for testing plans and documenting results

- methods and tools for capturing and maintaining the list of files and databases that constitute vital records (*Refer to the Knowledge and Information Management process area.*)

SC:GG2.GP4 Assign Responsibility

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

Elaboration:

SC:SG1.SP1 requires that the plan for managing service continuity address the roles and responsibilities for carrying out the plan and the program. SC:SG1.SP2 establishes standards and guidelines, including plan ownership and responsibility. SC:SG6 calls for identifying who is responsible for initiating action in any service continuity plan. In generic practice SC:GG2.GP4, resources are formally identified and assigned to plan elements.

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

Subpractices

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

Elaboration:

Responsibility and authority for performing service continuity 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 service and asset owners to participate in and derive benefit from the process for services and assets under their ownership or custodianship
- including process activities in staff performance management goals and objectives, with requisite measurement of progress against these goals
- developing and implementing contractual instruments (including service level agreements) with external entities to establish responsibility and authority for performing process tasks on outsourced functions
- including process tasks in measuring performance of external entities against contractual instruments

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

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

SC:GG2.GP5 Train People

Train the people performing or supporting the service continuity process as needed.

Elaboration:

SC:SG3.SP5 describes the activities necessary to develop and conduct effective service continuity training that conveys the contents of plans to those responsible for their execution. This specific practice also calls for identifying and filling service continuity skill gaps and needs before service continuity plans are validated.

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 service continuity process:

- knowledge necessary to elicit and prioritize stakeholder requirements and needs and interpret them to develop service continuity plans and programs, including the process plan
- knowledge required to develop service continuity plans
- communication skills for conveying the contents of service continuity plans to stakeholders
- knowledge unique to each type of service that is required to develop service-specific continuity plans
- knowledge necessary to work effectively with service and asset owners and custodians
- knowledge necessary to plan and conduct service continuity testing
- knowledge of the tools, techniques, and methods necessary to perform the process using the selected methods, techniques, and tools identified in SC:GG2.GP3 subpractice 3

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

3. Identify training opportunities to address skill gaps.

Elaboration:

Certification training is an effective way to improve service continuity skills and attain competency. Certifications such as the Business Continuity Certified Planner, Certified Specialist, and Certified Expert and the Certified Business Continuity Professional are available for staff who focus specifically on continuity planning and execution.

These are examples of training topics:

- service continuity plan development

- service continuity plan testing and revision
- change control for service continuity plans
- communicating service continuity plans
- conducting post-execution reviews
- identifying and resolving plan conflicts
- including external entities in plan development and execution

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

SC:GG2.GP6 Control Work Products

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

Elaboration:

SC:SG7.SP2 addresses the change control process over service continuity plans, including establishing criteria for making changes to plans. However, other work products of the service continuity process (such as the service continuity process plan and service continuity process policies) must also be managed and controlled. Tools, techniques, and methods should be employed to perform consistent and structured version control over service continuity plans to ensure that all who must rely on a plan have the most current and “official” version. The tools, techniques, and methods can also be used to securely store the service continuity plans, to provide access control over inquiry, modification, and deletion, and to track version changes and updates.

These are examples of service continuity work products placed under control:

- process guidelines and standards
- the plan for the process
- service-specific continuity plans
- business impact analysis results
- prioritized list of high-value services and associated assets
- list of public service providers, business partners, vendors, and other external entities
- key contacts lists
- files and databases that support high-value service operation, such as orders of succession and delegations of authority
- service continuity plan inventory/database
- service continuity plan test plans, standards, and schedule
- testing results
- training strategy, materials, and records
- change criteria for service continuity plan changes
- results of live service continuity plan execution
- policies and procedures
- contracts with external entities

SC:GG2.GP7 Identify and Involve Relevant Stakeholders

Identify and involve the relevant stakeholders of the service continuity process as planned.

Elaboration:

Several SC-specific practices address the involvement of stakeholders in the service continuity process. For example, SC:SG1.SP1 describes obtaining commitments to the plan for service continuity from service stakeholders. SC:SG1.SP2 requires that standards and guidelines address the identification and involvement of stakeholders. SC:SG3.SP2 calls for stakeholder identification for communication and review of service-specific continuity plans. Generic practice SC:GG2.GP7 generically covers the role of stakeholders throughout the service continuity process.

Subpractices

1. Identify process stakeholders and their appropriate involvement.

Elaboration:

SC:SG3.SP2 requires that stakeholders for service-specific continuity plans be identified and that plans be communicated to them. Subpractice 3 provides a list of examples of relevant stakeholders.

These are examples of stakeholders of the service continuity process:

- owners of high-value services and supporting assets (for which plans must be developed)
- custodians of high-value services and supporting assets (who may need to execute or participate in plans)
- organizational unit and line of business managers responsible for high-value services and supporting assets
- staff involved in developing plans
- external entities on which service continuity plans are dependent, such as public emergency management staff and other public agencies, partners, and suppliers
- external entities responsible for managing high-value services
- external entities to which the organization is a supplier
- regulatory and legal entities to which the organization is required to submit service continuity plans
- staff involved in versioning, storing, archiving, and securing plans
- staff involved in testing plans
- internal and external auditors

Stakeholders are involved in various tasks in the service continuity process, such as

- planning for the process
- making decisions about the process
- making commitments to service continuity plans and activities as well as the process plan
- developing service continuity plans and the process plan
- communicating service continuity plans and activities and process plans and activities

- coordinating process activities
 - participating in the test and execution of service continuity plans
 - reviewing and appraising the effectiveness of process activities
 - establishing requirements for the process
 - 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.

SC:GG2.GP8 Measure and Control the Process

Measure and control the service continuity process against the plan for performing the process and take appropriate corrective action.

Elaboration:

SC:SG5.SP4 requires that the results of service continuity plan testing be evaluated to determine if plans accomplished their objectives and met service continuity requirements, standards, and guidelines and produced test results as expected. SC:SG6.SP2 calls for post-execution review of service continuity plans that have been executed to ensure that plan objectives and expectations were met.

In generic practice SC:GG2.GP8, the service continuity process is formally monitored to ensure it is performing in accordance with the process plan.

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 service continuity process:

- elapsed time since the organization-wide plan for managing SC and the standards and guidelines for SC were reviewed and updated
- percentage of unstaffed roles and responsibilities in the organization-wide plan for managing SC
- percentage of SC guidelines and standards that are more/less stringent than required to meet compliance obligations

- number of relationships, e.g. internal and external dependencies or interdependencies, necessary to ensure SC
- number of points of contact for relationships that require updates
- elapsed time since review and update of the list of vital organizational records and databases
- percentage of SC plans completed
- number of required SC plans that have not yet been developed (based on high-value services and associated assets that do not have SC plans)
- percentage of SC plans that are not stored in a central storage system
- percentage of plans that are dependent on other plans; number of plans on which they are dependent
- percentage of plans with missing components (designated owner, resources, etc.)
- percentage of plans without established owners
- percentage of plans without identified stakeholders
- number of staff assigned to SC plans that are no longer employed by the organization
- percentage of defined roles in SC plans that are not assigned to specific staff
- percentage of defined roles in SC plans for which backup staff are not identified
- percentage of SC plans that do not meet service and asset resilience requirements
- percentage of SC plans that do not meet standards and guidelines
- percentage of staff not covered by a service continuity plan
- percentage of staff who have not been trained on their roles and responsibilities as defined in SC plans
- percentage of plans with one or more severe conflicts (such as a single point of failure) that have not been mitigated
- percentage of SC plans that do not have a schedule for testing and review
- percentage of SC plans that do not have a test plan
- percentage of SC test plans that have/have not been exercised
- percentage of interdependent service continuity plans that have/have not been jointly tested
- percentage of SC test plans that have failed one or more test objectives
- percentage of SC plan test objectives (RTOs and RPOs) unmet
- number of staff with defined roles in SC plans who do not have access to such plans within specified thresholds (time)
- average time for staff with defined SC plan roles to access SC plans
- percentage of realized risks for service continuity that exceed established risk parameters
- percentage of SC plans executed (never executed)
- percentage of plans that have not been reviewed post-execution
- percentage of plans that require changes (as defined by change criteria)
- percentage of plans that have been changed without authorization
- percentage of plans that have been changed without review
- percentage of plans that have been changed without testing

- frequency of changes to plans by service or service type

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 service continuity process are needed to ensure that

- the process is a planned and coordinated activity
- process planning is driven by managing and mitigating organizational risk
- internal and external dependencies that affect the process and service continuity plans are identified and considered
- vital organizational records are identified
- all service continuity plans have assigned owners
- service continuity plans are developed, resourced, and validated for high-value services, including new services that are developed or acquired
- service continuity plans are tested when developed and periodically as dictated by business conditions and the need to manage risk
- changes to service continuity plans and the plan inventory/database are controlled
- access to service continuity plans is limited to authorized staff
- the effectiveness of service continuity plans is measured
- the process is improved based on testing and experience in executing plans
- status reports are provided to appropriate stakeholders in a timely manner
- process 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.
7. Track corrective action to closure.

SC:GG2.GP9 Objectively Evaluate Adherence

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

Elaboration:

These are examples of activities to be reviewed:

- developing a plan for the process
- developing process guidelines and standards
- performing risk-based activities such as business impact analysis
- identifying service-specific continuity plans to be developed
- identifying external dependencies
- validating service continuity plans
- developing and testing service continuity plans
- making and managing changes to service continuity plans based on test results and as needs dictate
- storing, securing, and enforcing authorized access to service continuity plans
- performing post-event review of service continuity plans in execution
- the alignment of stakeholder requirements with service continuity plans and 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
- use of process work products for improving strategies for protecting and sustaining services and assets

These are examples of work products to be reviewed:

- the plan for the process
- process guidelines and standards
- service-specific continuity plans
- business impact analysis results
- lists of public agencies and other external entities, including business partners and vendors
- service continuity test plans
- testing results
- training records
- change criteria for plan changes
- service continuity plan change logs
- process plan and policies
- process issues that have been referred to the risk management process
- process methods, techniques, and tools

- metrics for the process (*Refer to SC:GG2.GP8 subpractice 2.*)
- contracts with external entities

SC:GG2.GP10 Review Status with Higher Level Managers

Review the activities, status, and results of the service continuity 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.

SC:GG3 Institutionalize a Defined Process

Service continuity is institutionalized as a defined process.

SC:GG3.GP1 Establish a Defined Process

Establish and maintain the description of a defined service continuity 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 service continuity 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.

SC:GG3.GP2 Collect Improvement Information

Collect service continuity 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:

SC:SG5.SP4 requires that the results of service continuity plan testing be evaluated to determine if plans accomplished their objectives, met service continuity requirements, standards, and guidelines, and produced test results as expected. SC:SG6.SP2 calls for post-execution review of service continuity plans that have been executed, to ensure that

plan objectives and expectations were met. Both of these specific practices and their work products may provide useful improvement information.

These are examples of improvement work products and information:

- results of business impact analysis
- issues related to service continuity plan development
- issues related to involving stakeholders in the development and execution processes
- issues related to committing to plan ownership and custodianship
- service continuity plan test results
- issues related to external entities
- issues related to internal and external dependencies and interdependencies
- conflicts arising from resource contention between service continuity plans
- lessons learned from plan testing
- lessons learned from plan execution
- metrics and measurements of the viability of the process (*Refer to SC:GG2.GP8 subpractice 2.*)
- changes and trends in operating conditions, risk conditions, and the risk environment that affect service continuity plans and process results
- lessons learned in post-event review of incidents and disruptions in continuity
- 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.