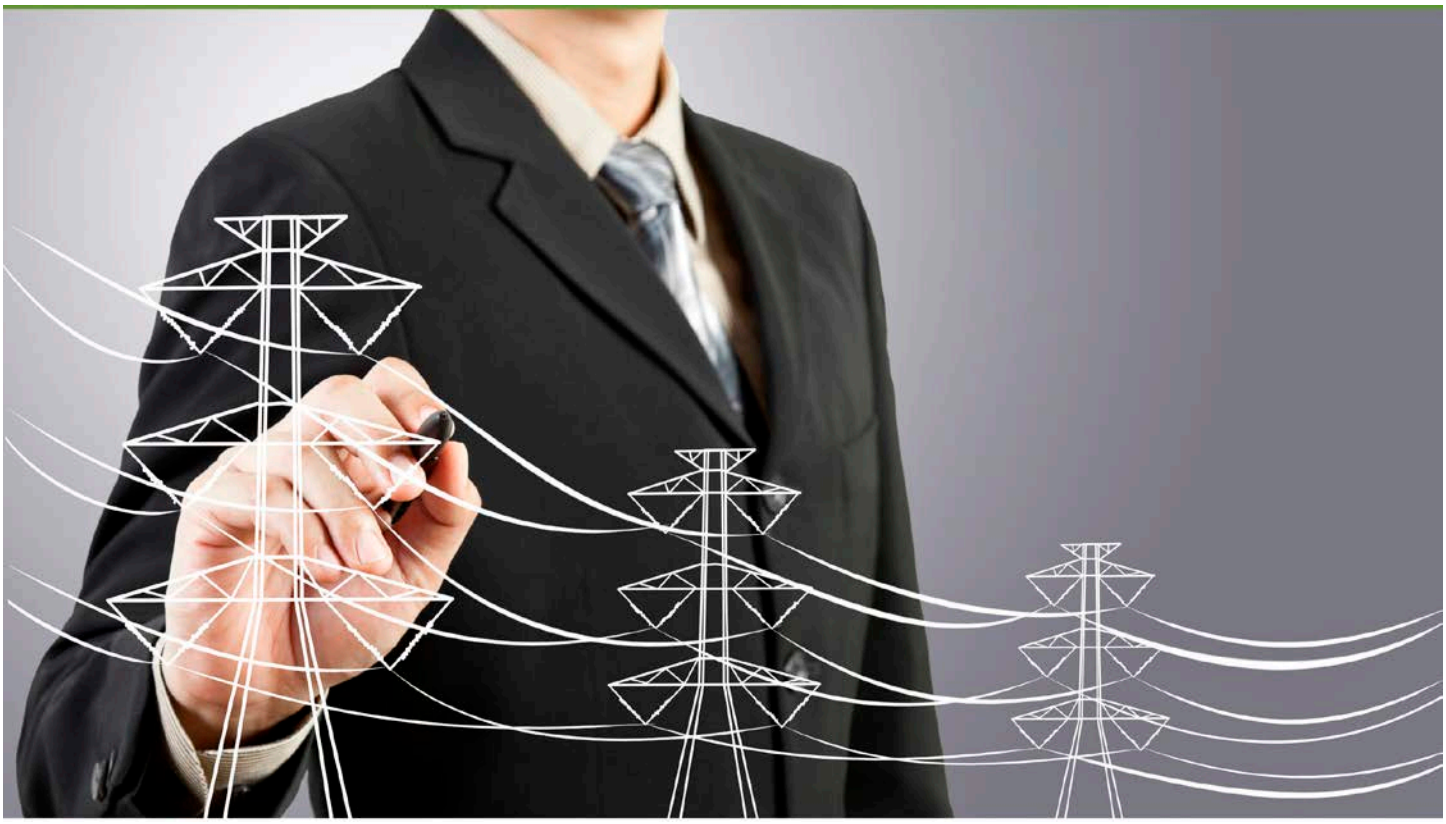
CRR Supplemental Resource Guide



Volume 6

Service Continuity Management

Version 1.1

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

DM-0003281

Table of Contents

I. Introduction

Series Welcome

Welcome to the CRR Resource Guide series. This document is 1 of 10 resource guides developed by the Department of Homeland Security's (DHS) Cyber Security Evaluation Program (CSEP) to help organizations implement practices identified as considerations for improvement during a Cyber Resilience Review (CRR).[1] The CRR is an interview-based assessment that captures an understanding and qualitative measurement of an organization's *operational resilience*, specific to IT operations. Operational resilience is the organization's ability to adapt to risk that affects its core operational capacities.[2] It also highlights the organization's ability to manage operational risks to critical services and associated assets during normal operations and during times of operational stress and crisis. The guides were developed for organizations that have participated in a CRR, but any organization interested in implementing or maturing operational resilience capabilities for critical IT services will find these guides useful.

The 10 domains covered by the CRR Resource Guide series are

1. Asset Management
2. Controls Management
3. Configuration and Change Management
4. Vulnerability Management
5. Incident Management
6. **Service Continuity Management** ⇦***This guide***
7. Risk Management
8. External Dependencies Management
9. Training and Awareness
10. Situational Awareness

The objective of the CRR is to allow organizations to measure the performance of fundamental cybersecurity practices. DHS introduced the CRR in 2011. In 2014 DHS launched the Critical Infrastructure Cyber Community or C³ (pronounced "C Cubed") Voluntary Program to assist the enhancement of critical infrastructure cybersecurity and to encourage the adoption of the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF). The NIST CSF provides a common taxonomy and mechanism for organizations to

1. describe their current cybersecurity posture
2. describe their target state for cybersecurity
3. identify and prioritize opportunities for improvement within the context of a continuous and repeatable process
4. assess progress toward the target state
5. communicate among internal and external stakeholders about cybersecurity risk

The CRR Self-Assessment Package includes a correlation of the practices measured in the CRR to criteria of the NIST CSF. An organization can use the output of the CRR to approximate its conformance with the NIST CSF. It is important to note that the CRR and NIST CSF are based on different catalogs of practice. As a result, an organization's fulfillment of CRR practices and capabilities may fall short of, or exceed, corresponding practices and capabilities in the NIST CSF.

Each Resource Guide in this series has the same basic structure, but each can be used independently. Each guide focuses on the development of plans and artifacts that support the implementation and execution of operational resilience capabilities. Organizations using more than one Resource Guide will be able to leverage complementary materials and suggestions to optimize their adoption approach. For example, this Service Continuity Management (SCM) guide suggests that a contact list be developed to support response and recovery. The information in that list can also be used as a starting point when developing the contact list recommended by the Incident Management guide. Other examples of materials that can be leveraged between guides include the scoping of specific implementation activities and the identification of key stakeholders.

Each guide derives its information from best practices described in a number of sources, but primarily from the CERT® Resilience Management Model (CERT®-RMM).[3] The CERT-RMM is a maturity model for managing and improving operational resilience, developed by the CERT Division of Carnegie Mellon University's Software Engineering Institute (SEI). This model is meant to

- guide the implementation and management of operational resilience activities
- converge key operational risk management activities
- define maturity through capability levels
- enable maturity measurement against the model
- improve an organization's confidence in its response to operational stress and crisis

The CERT-RMM provides the framework from which the CRR is derived—in other words, the CRR method bases its goals and practices on the CERT-RMM process areas.

This guide is intended for organizations seeking help in establishing a service continuity process and for organizations seeking to improve their existing service continuity process. To outline this process, this document will use an approach common to many service continuity standards and guidelines. The process areas described include

- Program
- Plan
- Validate and Exercise
- Improve

More specifically this guide

- educates and informs readers about the service continuity process
- promotes a common understanding of the need for a service continuity process
- identifies and describes key practices for service continuity
- provides examples and guidance to organizations wishing to implement these practices

Additionally, Appendix E provides a mapping between the practices that constitute SCM in the CRR and the appropriate Function, Category, and Subcategory in the NIST CSF.

® CERT® is a registered mark owned by Carnegie Mellon University.

The guide is structured as follows:

I. Introduction—Introduces the *CRR Resource Guide* series and describes the content and structure of these documents.

II. Service Continuity—Presents an overview of the service continuity process and establishes some basic terminology.

III. Establish and Maintain a Service Continuity Program—Outlines a program creation process and identifies issues and considerations to help ensure that the program addresses the organization's needs.

IV. Perform Service Continuity Planning—Provides a step-by-step approach to developing continuity plans following the approach developed in Section III.

V. Validate and Exercise Service Continuity Plans—Outlines the process for ensuring that the organization's service continuity plans meet standards set by the organization; outlines the process of exercising service continuity plans.

VI. Improve Service Continuity—Outlines the process and considerations for improving the service continuity program as well as plans.

VII. Conclusion—Provides a summary of service continuity references for further information.

Appendices

A. Example Business Impact Analysis Template
B. Example Service Continuity Plan Template
C. Example Service Continuity Plan Exercise Template
D. Service Continuity Resources
E. CRR/CERT-RMM Practice/NIST CSF Subcategory Reference

Audience

The principal audience for this guide includes individuals responsible for managing service continuity programs or mitigating business disruptions, including executives who establish policies and priorities for service continuity management, managers and planners who are responsible for converting executive decisions into plans, and operations staff who implement the plans and participate in the response to disruptive cybersecurity incidents.

To learn more about the source documents for this guide and for other documents of interest, see Appendix D.

II. Service Continuity

Overview

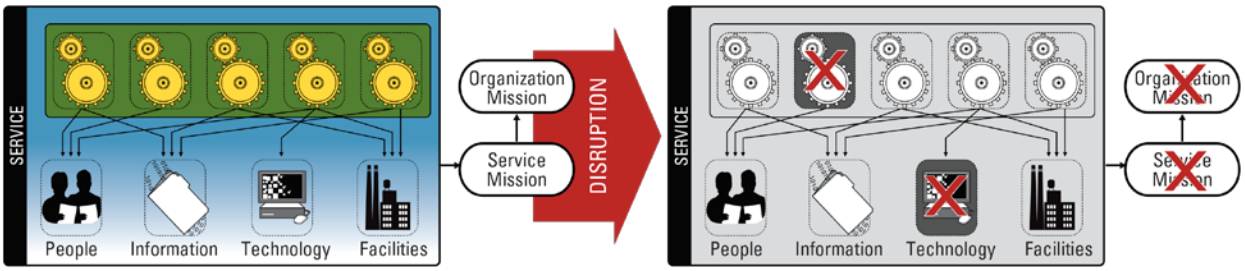


Figure 1: Disruption

Service continuity planning is one of the more important aspects of resilience management because it provides a process for preparing for and responding to disruptive events, whether natural or man-made. Operational disruptions may occur regularly and can scale from so small that the impact is essentially negligible to so large that they could prevent an organization from achieving its mission (see Figure 1). Services that are most important to an organization's ability to meet its mission are considered essential and are focused on first when responding to disruptions. The process of identifying and prioritizing services and the assets that support them is foundational to service continuity and will be addressed in the business impact analysis (BIA) discussion in Section III, Step 3.

Service continuity planning provides the organization with predefined procedures for sustaining essential operations in varying adverse conditions, from minor interruptions to large-scale incidents. For example, a power interruption or failure of an IT component may necessitate manual workaround procedures during repairs. A data center outage or loss of a business or facility housing essential services may require the organization to recover business or IT operations at an alternate location.

The process of assessing, prioritizing, planning and responding to, and improving plans to address disruptive events is known as service continuity. The goal of service continuity is to mitigate the impact of disruptive events by utilizing tested or exercised plans that facilitate predictable and consistent continuity of essential services. To accomplish this goal, an organization establishes processes that

- establish the service continuity program
- perform service continuity planning
- validate and exercise or test service continuity plans[4]
- improve service continuity

Figure 2 depicts the service continuity process.

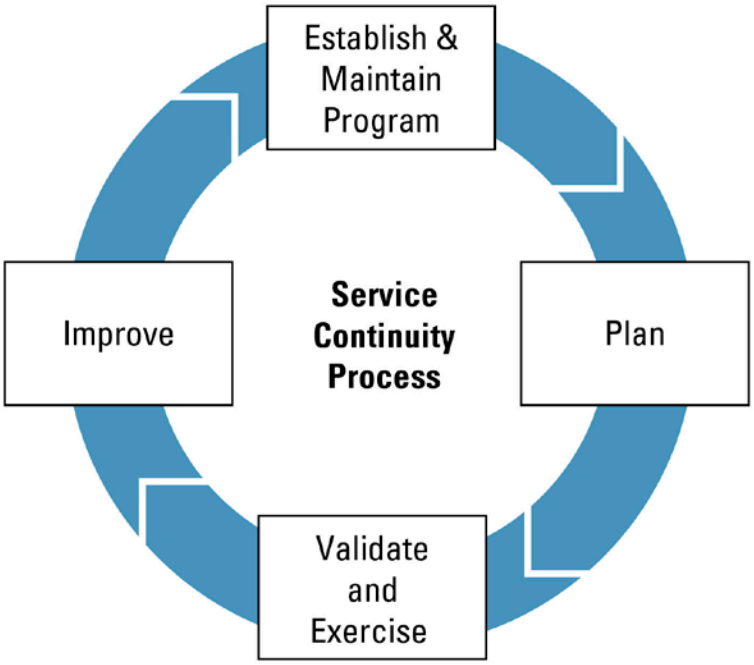


Figure 2: The Service Continuity Management Process

The following sections detail each of the steps in the service continuity process.

Establish and Maintain Program

A service continuity program provides the structure for

- developing responses to disruptions
- assessing disruption risk and the impact of disruptions on essential services
- overseeing the ongoing activities to plan, implement, exercise, and improve the service continuity process

The purpose of the continuity plans is to proactively determine and document the appropriate actions in the event of a disruption. The organization should develop continuity plans as part of implementing strategies for protecting its assets and sustaining its services. Service continuity requirements should be considered in the design of new services and systems whenever possible.

> *Service continuity focuses on proactively managing disruption risk to protect and sustain key assets to ensure the organization can achieve its mission. To be fully effective and efficient, service continuity requirements should be built into new services and systems.*

Ownership of the continuity plans should be at a level close to the management of the service, such as the service, unit, or business owner, so the plan can be revised as changes occur and improvement opportunities are identified. Organizations are dynamic, and changes in objectives, services, procedures, systems, staffing, and other aspects are more the norm than the exception. Ownership of the plan by a service, unit, or business owner clarifies accountability for ensuring that plans are updated and effective.

Keeping the plan current is an important practice, but exercising it is the most important practice for ensuring that the plan is effective and meets the organization's needs. Exercises are the best measure of plan quality and provide valuable opportunities to ensure its viability and train those who use it.

The following are the core foundational activities in the establishment and maintenance of the program:

- Ensure support for service continuity planning.
- Manage program design and supporting documentation.
- Oversee the BIA process.
- Monitor service continuity training and awareness activities.
- Establish linkages to the incident response and recovery process.

See the Incident Response Resource Guide, Volume 5 of this series, for more detailed guidance on that process.

Plan

Continuity plans document a set of actions an organization will take in response to a disruption. The core of planning is the identification of services essential to the organization and the establishment of service continuity requirements that reflect organizational needs and guide the recovery process during disruptions. Plans must be capable of addressing impacts to the core assets—such as people, technology, information, and facilities—that support the essential services. These key first steps of the planning process typically draw on a variety of organizational resources, including executives, unit and business leaders, technology support groups, and risk managers.

Because continuity planning is a risk management activity, it depends heavily on the requirements developed by the BIA and risk assessment processes described in Section III, Step 3. The type and content of the plans developed depend on the objectives of the organization, technology utilized, availability targets, risk tolerance, and budget constraints.

Continuity plans should have sufficient detail to be actionable. Some or all key trained personnel may not be available when plans must be executed, so plans should be detailed enough that unpracticed personnel can carry them out.

Continuity plans may take many forms. The structure of continuity plans varies and is influenced by a number of variables, including the organization's size, industry, and regulatory landscape. In some cases, one large integrated plan may accomplish the organization's planning needs in a single document. In other cases, the organization may develop many complementary documents that together meet its continuity needs. Examples of continuity plan types include

- business continuity plans—focus on the continued provision of essential services under degraded circumstances
- technology recovery plans—focus on recovery of essential applications, network communications, and technology infrastructure
- infectious disease or pandemic plans—focus on people and the continued provision of essential services during regional or global outbreaks of illness, most typically flu epidemics
- facility or data center recovery plans—focus on workspace and essential infrastructure

The goal is a continuity plan that works—a plan that can facilitate the effective delivery of the organization's essential services following a disruption. Plan format, name, size, structure, and other characteristics can be adjusted to fit the organization's culture, needs, and approach.

The following are the key activities in the service continuity planning process:

- Identify plans to be developed.
- Develop service continuity plans.

- Assign staff.
- Establish a service continuity plan repository.
- Define procedures for service continuity plan activation and execution.

Validate and Exercise

Before the organization can rely on its continuity plans, it should validate them to ensure they meet expectations. Continuity plans must be objectively reviewed to confirm that they achieve the resilience requirements for the covered services and assets. To establish plan consistency, accuracy, completeness, and effectiveness, the continuity plans should initially be examined against the standards and guidelines for plan development. All constituent plans should be reviewed together to identify any resource conflicts or other potential bottlenecks. This examination ensures consistent levels of documentation and the ability of the plans to meet stated objectives. It also reviews the logic of the plans and provides an opportunity to correct inconsistencies or gaps before resources are put at risk in plan exercise or execution.

The organization should develop an exercise strategy that outlines how exercises will be managed, including rigor, frequency, stakeholder involvement, and the number and type of units that should exercise together. Depending on the objectives of the continuity program, an oversight group might best manage the exercise strategy.

Exercises are the preferred method for validating continuity plans. Plans can be validated by executing them during a real event, but any problems in the plans could have a serious or catastrophic impact during an actual disruption. Exercises allow the organization to discover and make any necessary improvements to the plan before it is needed. Exercises also provide invaluable training to those involved so that they know their roles and responsibilities before an event.

A plan that has not been exercised is at high risk of not meeting objectives. Plan exercises are a critical step in promoting preparedness.

Exercises provide a valuable opportunity to train staff on the plan and service continuity, though training should be provided through a variety of vehicles. Training and plan awareness are some of the most important aspects of preparedness and should be carefully managed and monitored.

The following are the key activities of plan validation and exercise:

- Establish a plan review process.
- Develop an exercise strategy, process, and schedule.
- Exercise/execute service continuity plans.
- Evaluate exercise/execution results.
- Conduct an after-action review of plan activations and execution.
- Perform service continuity training.

Improve

Service continuity programs require careful management and review to help ensure they can effectively manage the risks associated with disruption. The organization should regularly review the program's strategies, standards, methodologies, and approach to ensure they are not only effective but also meet the organization's resilience management needs.

Changes in the operating environment, such as staff changes, evolving business processes, and newly identified risks, may require the organization to modify its service continuity plans and strategies. Exercising or executing an organization's continuity plans might also reveal needed updates. As material changes occur to the operations or the organization, service continuity plans should be updated; typically a review of plans is required at least annually.

In addition to change, dependencies and interconnectedness are a fundamental challenge faced by organizations when developing service continuity plans. Developing exercise strategies to consider various scenarios and potential linkages to other internal and external groups provides a means of identifying plan improvements and maturing the organization's service continuity capabilities. Exercising plans with other groups and organizations is a leading practice and, for some, a regulatory requirement. When multiple plans must work together to facilitate an effective recovery, such as with interrelated business functions, infrastructure, applications, and vendors, the continuity plans must work in unison. Jointly exercising the plans is one of the best ways to ensure an integrated, effective recovery.

See the External Dependencies Management Resource Guide, Volume 8 of this series. Also see External Dependencies Management in the CERT Resilience Management Model for additional information on managing risks associated with external providers.[5]

The following are the key activities of service continuity program improvement:

- Review overall service continuity program effectiveness.
- Proactively identify conditions for revising service continuity plans.
- Make improvements.

Plan for Service Continuity

Having a defined program and processes for creating, validating, and improving service continuity plans provides consistent, predefined procedures for sustaining critical services to help ensure that an organization's mission-critical objectives are met during an operational disruption. Without a defined process, an organization might omit actions that are critical to sustaining or recovering operations. A service continuity plan describes the actions an organization will take to respond to operational disruptions.

The following sections of this guide lay out the discrete steps for developing a plan that implements the service continuity program as described above:

Establish and Maintain a Service Continuity Program

1. Ensure support for service continuity planning.
2. Manage program design and supporting documentation.
3. Oversee the business impact and risk assessment process.
4. Monitor service continuity training and awareness activities.
5. Establish linkages to the incident response and recovery process.

Perform Service Continuity Planning

1. Identify plans to be developed.
2. Develop continuity plans.
3. Assign staff.
4. Establish a service continuity plan repository.
5. Define procedures for service continuity activation and execution.

Validate and Exercise Service Continuity Plans

1. Establish a plan review process.
2. Develop an exercise strategy, process, and schedule.
3. Exercise/execute service continuity plans.
4. Evaluate exercise/execution results.
5. Perform service continuity training.

Improve Service Continuity

1. Conduct exercises.
2. Proactively identify signs that the program and/or plans need to be revised and improved.
3. Make improvements.

Organizations that already have service continuity plans can use the guidance in this Resource Guide to assess and make improvements to the existing service continuity plans.

III. Establish and Maintain a Service Continuity Program

Before You Begin

The following checklist summarizes the tasks you will need to complete and the information you will need to gather before you can begin developing a service continuity program.

	Input	Guidance
✓	Scoping statement	This statement defines what the service continuity program and plans need to address. The plans could be scoped to cover, at a minimum, all mission-essential organizational services. Organizations that are not sure where to start should focus on the most essential services and the areas that directly affect their performance. This approach may allow an organization to address the areas of greatest risk first and mitigate their impact while service continuity practices are being more fully developed. If your organization has participated in a CRR, it may be beneficial to begin with the essential service addressed during the CRR. See Appendix E for a cross reference between the CRR and this guide.
✓	Lists of stakeholders	The list of stakeholders should be aligned to the scoping statement and include all appropriate internal and external entities. Potential candidates include • service/business owners within the organization • business partners and vendors • technology and infrastructure owners in the organization • law enforcement and other first-responder organizations • technology vendors • recovery partners (recovery services) • regulators and auditors • customers and providers who may be impacted in the event of service interruption
✓	Management support	An endorsement by senior management for establishing a service continuity program and implementing processes
✓	An understanding and acknowledgement of an acceptable approach to service continuity	Acknowledgement of the intended approach to service continuity, including stakeholder expectations about acceptable strategies and objectives
✓	Externally imposed requirements for service continuity	• Regulatory requirements defining mandatory continuity planning requirements and other needs • Service-level agreement requirements with other organizations where service continuity is required
✓	Assignment of responsibility for service continuity	Job descriptions and performance reviews for roles that have responsibilities for service continuity, for example, executive ownership, decisions, communication, testing, and disruption risk management

✓	Budget for service continuity	Identification of available funds and resources to perform service continuity: • staffing resources • tools (applications and associated hardware) • third-party support • technology to support resilience requirements
✓	Linkage to the incident management plan	Coordination of event, incident, and notification processes with service continuity planning, testing, and execution

Step 1. Ensure support for service continuity planning.

Service continuity requires support and commitment from the executive leaders in the organization due to the potentially widespread support requirements and nature of disruptive events, for example, hurricanes, earthquakes, and cyber attacks. Smaller events, while less geographically widespread, often require support from many areas of an organization to be effective, such as multiple related business areas, technology teams, facilities, human resources, legal, and public relations. To help ensure that service continuity has the necessary level of commitment and engagement, it is essential that some kind of oversight or steering group be established. The oversight or steering group is best composed of business and technical leaders from across the organization. The process also benefits from the involvement of or linkages to other risk and oversight groups, such as the organizational functions of audit, operations risk, compliance, and boards of directors. For more heavily regulated organizations, such involvement is required.

Managing disruptions and service continuity are foundational risk management activities, making senior-level support and commitment essential to establishing a strong program.

Step 2. Manage program design and supporting documentation.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Reference
Goal 1: Service continuity plans for high-value services are developed.	
2. Are service continuity plans developed using established standards, guidelines, and templates? [SC:SG3.SP2]	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.

A. Establish policy and standards for service continuity. A clear business rule or policy should establish the need for a service continuity program.[6] The policy and supporting documents provide a foundation for ensuring that the organization considers disruption risk and that investments in the service continuity program provide adequate support to meet the resilience requirements and risk tolerance of stakeholders. Standards that provide detailed requirements help establish clear direction for the organization. Standards clarify the content that should be included in documentation and facilitate the use of a common format for that information. Standards for plans may require specific content, such as facility names and locations, server names, number of people affected by the plan, type of office equipment used, and names and contacts at key vendors.

Example service continuity policy:
Each operating unit and/or business area will develop and conduct annual testing of a business continuity plan that supports the orderly recovery of essential services in the event of a major disruption or disaster.

Comprehensive service continuity standards may include

- a technology recovery plan
- a work area recovery plan

- exercise frequency
- exercise documentation
- alternate site requirements
- notification and escalation criteria

B. Develop service continuity program documentation. Service continuity program documentation helps to ensure that important elements of continuity are consistently understood, developed, and maintained by the personnel who are responsible for continuity activities. The documentation should include summary program information along with procedural information, templates, and tools to simplify the continuity planning process. Some examples of service continuity program documentation include

- service continuity program structure and overview
- program governance and oversight
- service continuity approach and strategies
- functional organization charts
- program objectives, short- and long-term
- risk assessment and BIA procedures and template(s)
- oversight of and coordination with essential vendors and external suppliers
- plan review, approval, and maintenance procedures
- plan repository requirements, location, and usage instructions
- metrics design and reporting

C. Create templates and guidelines for service continuity. Templates and guidelines help ensure that common, important elements of continuity are consistently utilized over time by the personnel who are responsible for continuity activities. Establishing common templates and guidelines not only simplifies the continuity planning process but also helps manage disruption risk in a manner that meets organizational goals. Templates and guidelines typically include

- business continuity plans
- technology recovery plans
- infectious disease/pandemic plans
- versions of plans to address improvements, maintenance, and approval
- contact lists and notification-escalation procedures
- review and approval process

Step 3. Oversee the business impact analysis process.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Reference
Goal 1: Service continuity plans for high-value services are developed.	
1. Are service continuity plans developed and documented for assets required for delivery of the critical service? [SC:SG3.SP2]	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.
6. Are availability requirements such as recovery time objectives and recovery point objectives established? [TM:SG5.SP1]	ID.BE-5: Resilience requirements to support delivery of critical services are established.
	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.

The BIA is a foundational element of a service continuity program. The BIA measures the effects of a disruption on an organization's services and how they impact changes over time.

A. Define business impact analysis characteristics.

i. The BIA considers the impact of disruptions over time and provides requirements for the development of continuity plans. Consider the best time frames for capturing impact, for example, four hours, one day, two days, or even days, weeks, or months.

ii. The BIA is the key process tool used to establish continuity requirements and prioritize business services' importance to meeting an organization's mission. Consider the requirements that should be collected—for example, resources required and their relative importance.

iii. The BIA identifies what to recover and when that recovery needs to be completed. Consider which services must be up and running and by when.

B. Establish a link to risk assessments. Risk assessments help identify the key exposures to consider in the BIA by providing insights into the likelihood and potential impact of various disruption threats, whether natural or man-made. Leverage existing risk assessments that the organization may have conducted to

i. obtain input to the BIA and integrate with evaluation and mitigation activities already underway. Typically groups involved in operational risk, enterprise risk, finance, audits, or compliance are good sources of information on previous risk assessments.

ii. identify the essential services of the organization. Previous risk assessment documentation or senior leaders can be consulted when establishing this list.

iii. determine the priority of services that are most essential or that need to get back online fastest in the event of a disruption. Service owners, managers, and senior leadership are good sources for establishing priorities.

C. Determine how to measure the impact of a service disruption. Impact information is usually measured in dollars, customers affected, reputational impact, and regulatory noncompliance. These measures of impact can inform the development of continuity requirements and strategies. In many instances, organizations look to the BIA information to develop a business case for investment in mitigation activities. This strategy aspect of continuity planning is a core driver of continuity process management. Organizations doing continuity planning must weigh spending and investment against risk. The continuity strategy decision process can clarify the risk tolerance of the organization, for example, a willingness to accept the risk of longer recovery times to keep costs down.

See Appendix A for a BIA template. See the Resources list in Appendix D for a number of other sources of BIA templates and information.

D. Identify the required information in a BIA for each service assessed. The BIA process typically provides the following requirements and priorities for essential services:

- recovery time objective (RTO)—desired speed of recovery
- recovery point objective (RPO)—desired currency of the information recovered
- essential services and priorities
- essential application and technology priorities
- critical facilities priorities
- critical information and data priorities
- critical people
- critical infrastructure and support processes

E. Identify information the BIA should collect to support the service continuity planning process. The BIA can also be used to collect information that supports broader organizational continuity planning and

strategy development. It may also identify areas for improvement in organizational processes and technology needed to support service continuity. Service continuity program information may include

- the identification of potential conflicts among plans
- the identification of gaps in supporting processes
- improved integration of plans among interconnected groups
- the development of shared continuity solutions for facilities, vendors, technology centers, and other upstream and downstream dependencies
- shared systems and applications
- shared recovery sites
- critical vendors or third-party suppliers
- technology sizing (e.g., dial-up connections to support work-at-home strategies)
- vital records locations and exposures

The BIA process and related discussions offer an excellent opportunity to provide continuity training and strengthen the preparedness awareness of an organization's key stakeholders and executives.

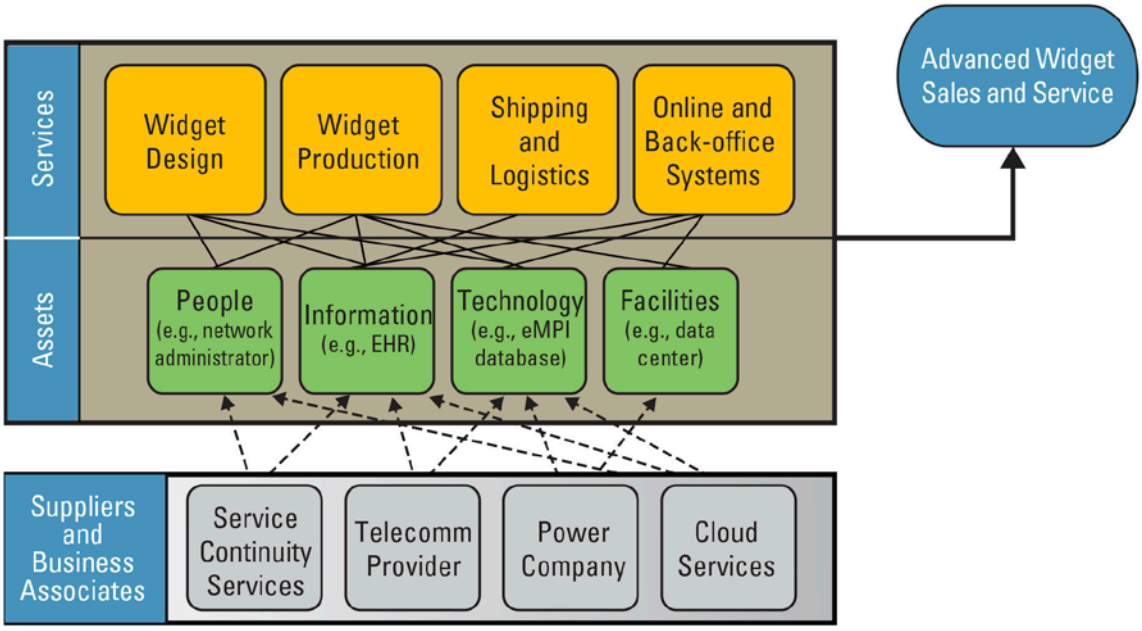


Figure 3: Service, Asset, and External Provider Relationships

F. Establish priority and recovery timing among essential services. Once documented, the lists of services, associated assets, and external dependencies can inform decisions about priorities and timing in continuity planning (see Figure 3). In abnormal situations, it may be necessary to forego or alter the execution of some services. To mitigate potential resource conflicts, organizations may need to operate other services in a store-and-catch-up-later mode.

Step 4. Monitor service continuity training and awareness activities.

Training and awareness for service continuity is a critical aspect of the overall program. Staff members should be aware of the continuity program, its general strategies, and any specific responsibilities they may have during a disruption.

The orientation process for all new employees and contractors should provide basic service continuity training. Specific training on service continuity plans or program responsibilities is often best provided in conjunction with exercises. Including a requirement for continuity training and participation in job descriptions can help ensure that the service continuity program receives effective support from trained and aware participants.

Step 5. Establish linkages to the incident response and recovery process.[7]

Service continuity plans provide the foundation for an organization to respond to physical or cyber disruptions. Developing the continuity plans at a business unit or regional level helps ensure that those most familiar with the essential services are engaged in planning for an organized, effective response to a disruption.

The overall organizational response to disruptions may require coordination and management that can be most effectively provided by multidisciplinary incident response teams. This is particularly true in the case of major incidents and larger organizations.

See the Incident Management Resource Guide, Volume 5 of this series, for more detailed guidance on that process.

Output of Section III

	Output	Guidance
✓	Enterprise guidance for service continuity	Organization-wide program, strategy, standards, and documentation for performing service continuity activities
✓	Executive endorsement and oversight of service continuity planning	Service continuity policy, standards, and a program oversight or steering group
✓	Identified stakeholders for service continuity	All participants in the service continuity process, including owners of services, will be aware of their roles and responsibilities
✓	Key foundational processes established	• Business impact and risk assessment processes defined to provide resilience requirements to the planning process • Training and awareness activities incorporated into job functions and employment processes
✓	Linkage to the incident management process established	Service continuity and incident management are complementary processes that must work closely together to help ensure resilience and the effective management of disruptions
✓	Identified laws, regulations, and rules	List of requirements affecting the organization's service continuity
✓	Service continuity procedures	A written description of how service continuity activities will be conducted throughout the organization
✓	Detailed processes for service continuity	Predefined processes for services continuity development, validation, exercising, execution, maintenance, and improvement

IV. Perform Service Continuity Planning

Before You Begin

The following checklist summarizes the tasks you will need to complete and the information you will need to gather before you can begin developing service continuity plans.

	Input	Guidance
✓	Planning statement	The planning statement provides direction and scoping for plan development. For example, plan development should eventually cover all mission-essential services but will begin with the single most critical service and proceed in descending order of criticality, as identified in the BIA. If your organization has participated in a CRR, it may be beneficial to begin with the critical service addressed during the CRR.
✓	Lists of stakeholders	The list of stakeholders should be aligned to the planning statement and include all appropriate internal and external entities. Potential candidates include • Incident Management Team, which typically notifies o first responders, such as law enforcement, fire, and medical o technology support vendors and recovery partners (i.e., disaster recovery services) o infrastructure providers, such as data, telephony, and regulatory agencies • executive and senior management for notification and escalation • other affected critical service owners • information technology service owners • owners of emergency funding and supporting logistics services • customers and providers who may be impacted by a service disruption • service recovery staff, including the critical service owner and response team members
✓	Management support	An endorsement by senior management for conducting service continuity planning activities and implementing processes
✓	Service continuity documentation	• Policy • Standards • Guidelines • Templates
✓	Externally imposed recovery requirements	• Regulatory requirements defining mandatory recovery parameters • Service-level agreement requirements
✓	Budget for service continuity planning	• Identification of available funds to perform service continuity planning and execution, including funds for o staffing resources o tools (applications and associated hardware) o third-party support

Step 1. Identify plans to be developed.

Comprehensive service continuity planning encompasses the four types of assets that make up a service: people, information, technology, and facilities. Organizations often develop continuity plans of different types, such as business continuity plans, technology recovery plans, and pandemic plans. These plans address the loss of the facility where the service is delivered, the technology and information that support the service, and the people who provide the service. The types of plans required depend on the needs and requirements of the individual organization.[8]

A. Prioritize services and plans to be developed. Mission-critical services should be prioritized based on the BIA, discussed in the previous section. The prioritization of critical services should drive the order in which continuity plans are developed. Organizations that have participated in a CRR may want to start with the critical service that was the focus of the CRR. Use the BIA data to

i. identify the critical services the organization provides
ii. prioritize development of plans for different service areas
iii. identify recovery requirements, such as RTOs, RPOs, and service-level agreements
iv. help identify recovery strategies (e.g., use of alternate site, use of manual work-arounds)

B. Select the type of plan or plans to develop for the service.

- **Business continuity plans.** Business continuity plans focus on critical business services. Services vary in number and type depending on the nature of each organization's mission. For example, organizations that are part of the national critical infrastructure (e.g., those that are the focus of CRRs) provide different critical services such as clean water, energy, food, and financial services. Multiple supporting activities may be essential to the delivery of the critical service. Business continuity plans typically address scenarios such as
  - loss or inaccessibility of the primary facility in which the service is provided
  - loss of supporting technology and the manual procedures to work around the loss
  - loss of people necessary to perform the service
- **Technology recovery plans.** Technology recovery plans may address all aspects of computer and information systems, as well as infrastructure control systems, supervisory control and data acquisition (SCADA) sysstems, or manufacturing systems. Technology recovery plans typically address scenarios such as
  - loss of a data center
  - loss of critical computer systems within a data center
  - loss of communications capability for which the organization is responsible
  - loss of capability due to a cyber incident
  - loss of collocated technology operations and business operations
- **Pandemic/infectious disease plans.** Pandemic plans deal with the potential widespread loss of people, typically caused by disease. Organizations usually have a pandemic plan that encompasses all of the organization's resources needed to deal with such a scenario, with supporting procedures in unit or business area plans. Pandemic planning has a few unique characteristics, including a focus on the people of the organization, broad potential global impacts, and the extended duration of the event. Pandemic planning is not the focus of this guide; rather this guide focuses on the personnel needed to deliver a specific critical service addressed by the business continuity plan.

Step 2. Develop service continuity plans.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Reference
Goal 1 – Service continuity plans for high-value services are developed.	
1. Are service continuity plans developed and documented for assets required for delivery of the critical service? [SC:SG3.SP2]	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.
2. Are service continuity plans developed using established standards, guidelines, and templates? [SC:SG3.SP2]	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.
4. Are key contacts identified in the service continuity plans? [SC:SG2.SP2]	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed. RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams. RS.CO-4: Coordination with stakeholders occurs consistent with response plans.
6. Are availability requirements such as recovery time objectives and recovery point objectives established? [TM:SG5.SP1]	ID.BE-5: Resilience requirements to support delivery of critical services are established. PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.

Continuity plans must be based on the requirements gathered in the BIA and include all relevant recovery requirements. If a BIA is not available, requirements gathering may begin by using other internal information, such as service-level agreements and risk assessments.

A. Start with your organization's guidelines and templates for the type of plan to be developed.

i. Guidelines, standards, and templates for developing plans are usually created during the establishment of the service continuity program, as described in Section III.[9] There are many resources for templates, such as local business continuity planning associations. Appendix B provides an example service continuity plan template.

ii. The guidelines, standards, and templates define the scope and approach to plan development, as identified above.

iii. If plan templates are not available, it will be necessary to create a plan format at this stage of the process.

See Appendix B for an example service continuity plan template.

B. Create the plan.

Table 1 lists the common components of continuity plans. Use this table as a starting point for developing continuity plans.

Table 1: Common Components of Continuity Plans

Component	Description
Alternate Site(s)	Identify the location(s) for any applicable alternate processing site for the service.
Assignment of Responsibility	Use functional responsibility descriptions instead of names to simplify plan maintenance.
Assignment of Team Members	List employees at your organization who are responsible for developing and maintaining the plan, including a notification list of primary and alternate team members for functional responsibilities.

Component	Description
Communication Protocols	The service continuity plan should include communication processes to identify • communications channels to be used to notify stakeholders and Incident Management contacts if this plan is executed • communication channels to be used to coordinate recovery activities
Continuity Plan Activation Criteria	Describe conditions that must be met before this continuity plan can be executed.
Essential Information Assets	List the information assets (data and paper-based vital records) essential to the service.
Essential Technology Assets	List the technology assets essential to the service.
Executive Support	List the executives who had input to this document and endorse its development and applicability.
Key Contacts	List the key contact information[10] essential to each service and this plan. Include the service owner as well as internal and external technical support, emergency contacts, and all relevant stakeholders.
Key Documentation	Identify technical manuals, reference guides, other supporting materials, and their offsite locations that may be necessary to restore service operations.
Laws, Regulations, and Rules	Identify and list legal requirements that your organization must consider when activating the plan.
Recovery Objectives	Identify the RTO for the service and relevant assets, along with the RPO for data and information.[11] Include regulatory requirements and business obligations, such as information about service-level agreements.
Recovery Procedures for the Service	List step-by-step instructions for recovering the service at the normal operating facility, as well as for recovering the service at the alternate processing facility.
Related Continuity Plans	Identify any continuity plans that affect or are affected by this continuity plan.
Roles and Responsibilities	Identify roles essential for restoring and performing the service.
Security or Access Issues	Identify security or access issues important to accessing the alternate sites or in case of plan activation outside of normal operating hours. Consider both physical and logical access.
Service Description	Explain or define the service to provide a high-level understanding to personnel who must implement this plan.
Service Owner(s)	List the business owner(s) responsible for the service(s), including contact information.
Service Priority	Indicate the priority of the service with respect to other services (BIA provides this information).
Special Considerations for Information Assets	Identify any special considerations for handling information assets in the event of plan activation, such as confidentiality or privacy requirements.
Exercise Requirements and Frequency for This Plan	Specify the frequency at which the plan must be exercised. Plans for highly critical services may need to be tested more often than general guidelines specify.
Type of Impact	Identify conditions for which specific responses are to be developed as the response actions. It is a best practice to plan for worst-case scenarios such as loss of a facility, supporting technology, or staff.

C. Identify dependencies and potential resource conflicts.[12] Dependencies among the plans must also be addressed to provide comprehensive service continuity. Organizations should consider, for example,

- upstream and downstream dependencies
  - internal and external services on which this critical service depends
  - services that depend on the recovery of this critical service
- vendor interaction and coordination
  - external suppliers
  - outsourced processes or operations that are part of the critical service
  - supporting technology vendors
- competition for resources
  - recovery staff
  - recovery space

  - technology
- potential implications of large regional disruptions
  - disaster declaration and vendor recovery site availability
  - actions of external authorities
  - restriction of support services and transportation
  - availability of communications channels
- managing targeted attacks on cyber or physical infrastructure
  - points of contact at law enforcement
  - your organization's priority in external response efforts
  - the external responder's authority over your organization's recovery efforts
- a list of external suppliers such as power, water, communications, and safety providers
  - redundancy of suppliers
  - alternate sources
- internal supporting resources
  - availability of financial resources
  - availability of logistics resources

Step 3. Assign staff.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Reference
Goal 1: Service continuity plans for high-value services are developed.	
3. Are staff members assigned to execute specific service continuity plans? [SC:SG3.SP3]	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.
	RS.CO-1: Personnel know their roles and order of operations when a response is needed.

The plan defines roles and responsibilities essential to its execution and that must be filled.[13]

A. Assign staff to roles identified in the plan. Considerations for matching personnel to continuity plan roles include
- alternative staff if the primary member is not available
- avoiding conflicting assignments to roles in your plan as well as conflicting assignments across plans for other services
- availability of each staff member during a disruption
- the necessity to physically relocate staff and constraints on their ability to travel
- qualifications to fill the role

B. Add service continuity responsibilities to job descriptions. Service continuity roles are often secondary or collateral duties. Adding these roles to job descriptions and performance metrics demonstrates the importance of their performance to the organization and provides a means of tracking necessary skills during staff turnover.

Step 4. Establish a service continuity plan repository.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Reference
Goal 1: Service continuity plans for high-value services are developed.	
5. Are service continuity plans stored in a controlled manner and available to all those who need to know? [SC:SG3.SP4]	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.

Service continuity plans are actionable only if they are up to date and available when needed. Establishing a repository provides an environment from which to manage the integrity and availability of the plans.[14] Considerations for a repository include

- access by recovery staff
  - real-time access to plans to support recovery
  - procedures for offsite or remote access if the repository is not available
- security of sensitive information
  - recovery location and procedures
  - private information of the recovery staff
- integrity of information
  - facilitate plan maintenance
  - role-based access
- availability and backup of the repository
  - required backup frequency to keep plans current[15]
  - alternate location if the repository is affected by the service interruption[16]

Step 5. Define procedures for service continuity plan activation and execution.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Reference
Goal 4: Service continuity plans are executed and reviewed.	
1. Have conditions been identified that trigger the execution of the service continuity plan? [SC:SG6.SP1]	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.
	RC.RP-1: Recovery plan is executed during or after an event.

Organizations should establish and document conditions under which service continuity plans are to be activated, who has the authority to activate plans, and the level of discretion in making the decision to activate.

A. Develop criteria for activating and executing each service continuity plan.

i. Criteria should be derived from the organization's policies, standards, and guidance for activating plans.

ii. Triggers for plan activation should be based on service interruption tolerance thresholds, RTOs, and RPOs as determined in the BIA,[17] for example,

- when normal processing is interrupted for longer than four hours and a return to normal operation is not assured within the next four hours
- in any case where normal processing has been unavailable for eight hours or more during normal operating hours
- when orders to evacuate are likely to extend beyond eight business hours
- as recommended by the county emergency management agency (or other regulatory body)

i. Authority to activate the plan and direct its execution should be specified by title and name, for example, executive officers, plan owners, IT director, and operations managers.

B. Develop communication procedures, including notification and escalation, to include

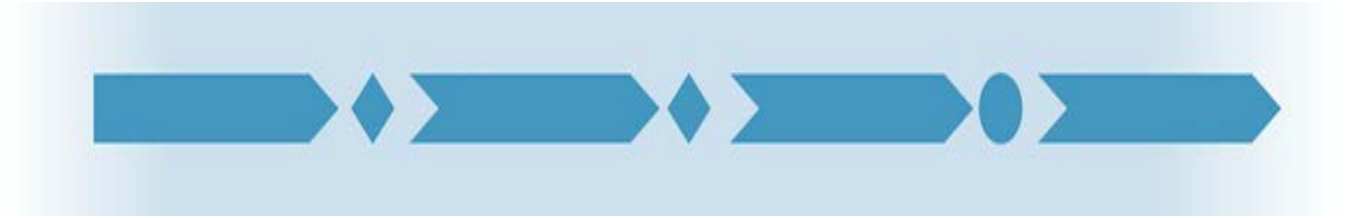
- internal communication to staff responsible for plan execution
- activation notification and communication with the organization's incident management team. If there is no incident management team, the organization should develop procedures to communicate with
  - other affected organizational services
  - first responders, such as law enforcement, fire, and medical
  - media, if authorized
- procedures for communicating internally and externally to parties affected by the plan activation and potentially the service interruption

C. Develop procedures for

i. recovery team status reporting
ii. updates to the incident management team, if necessary
iii. documentation of open items and issues in the recovery plan process
iv. closure of open items

Output of Section IV

	Output	Guidance
✓	Critical services	Critical services identified and prioritized
✓	Service continuity plans	Service continuity plans developed for critical services, including recovery expectation with procedures for recovery of business operations, technology, and staff
✓	Identified stakeholders for service continuity	All participants in the service continuity process are assigned to roles and aware of their responsibilities
✓	Plan repository	A secure location for storing and maintaining continuity plans that provides access and availability when plans are needed
✓	Plan activation criteria	Conditions under which a service continuity plan will be activated and the authority to activate the plan



V. Validate and Exercise Service Continuity Plans

Service continuity plans are not considered actionable until they have been validated by review, to ensure they meet the standards and guidelines set forth by the organization, and until they have been exercised, to ensure that the actions detailed in the plan will actually be effective in recovering the service.

Plans can be validated by executing them during a real event, but any problems in the plans could have a serious or catastrophic impact during an actual disruption. Exercises allow the organization to discover and correct any necessary improvements to the plan before it is needed.

The validation process is usually progressive and includes plan reviews, tabletop exercises, full-plan exercises, and integrated exercises of multiple plans.

This document uses the term exercise *instead of* test*, which has a pass/fail connotation. However,* test *is appropriate in some cases.*

Before You Begin

The following checklist summarizes the tasks you will need to complete and the information you will need to gather before you can begin reviewing and exercising service continuity plans.

	Input	Guidance
✓	Completed continuity plans	Continuity plans to be validated against standards and guidelines upon completion of their development
✓	Continuity planning standards and guidelines	Plan criteria, content, and required components
✓	Availability requirements for the service	The collection of business and regulatory obligations and tolerances identified and documented in the BIA for the service covered by the plan
✓	Approval and engagement from stakeholders	• Establish the scope and scenario of the exercise to be conducted • Establish the schedule of the exercise to be conducted • Determine the role of stakeholders in the exercise
✓	Selected service continuity plan(s) to be exercised	Identify plan(s) to be exercised
✓	The type of exercise to be conducted	• Identify the type to exercise to be conducted, i.e., tabletop, partial-function recovery, full-function recovery, or integrated recovery • Independent exercises of individual plans or integrated exercising of multiple plans • May use a progressive approach from tabletop to partial-function recovery or full-function recovery exercises
✓	Exercise objectives	Objectives should align with business strategy for critical services

✓	Reporting and data collection requirements	Standard reporting of exercise results to facilitate progress over time, as well as the types of exercises for comparison to other plan exercise results and the collection of the data necessary for reporting

Step 1. Establish a plan review process.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Reference
Goal 2: Service continuity plans are reviewed to resolve conflicts between plans.	
1. Are plans reviewed to identify and resolve conflicts? [SC:SG4.SP2]	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.
	RC.IM: Recovery planning and processes are improved by incorporating lessons learned into future activities.

Service continuity plans should be reviewed immediately upon the completion of their development to ensure that they meet the organization's criteria for putting the plans into service.

A. Plan reviews should cover at a minimum

- compliance with guidelines, standards, and templates
  - plan components
  - staff assignments
  - comprehensive coverage, such as loss of technology, people, and facilities
- linkage and coordination with upstream and downstream interdependencies, as described in Section IV, Step 2 C
- identification of conflicts for resources with other plans or within a plan
- review by the service continuity planning manager or team, if the organization has one
- review by the owner of the service covered by the plan, including business operations and technology

Plan reviews are a valuable step in the continuity process, but exercising the plans provides the most effective means to identify any gaps or needed improvements.

B. Plan approval. Service continuity plans should be approved by a senior manager, preferably one responsible for the delivery of the service. Approval may also occur after the plan has been exercised and has met objectives.

Step 2. Develop an exercise strategy, process, and schedule.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Reference
Goal 3: Service continuity plans are tested to ensure they meet their stated objectives.	
1. Have standards for testing service continuity plans been implemented? [SC:SG5.SP1]	PR.IP-10: Response and recovery plans are tested.
2. Has a schedule for testing service continuity plans been established? [SC:SG5.SP1]	PR.IP-10: Response and recovery plans are tested.

Organizations must have a strategy for exercising service continuity plans to ensure they are viable and effective at meeting the organization's resilience requirements.[18] The strategy should address how exercises will be conducted, the progression from simple to more complex exercises, type of exercise (e.g., tabletop, simulation, partial-function recovery, full-function recovery, and fully integrated), and the frequency of

exercises.[19] Figure 4 shows an example of a comprehensive exercise process, as defined by the Federal Emergency Management Agency (FEMA). An exercise should be tailored to fit your organization's needs.

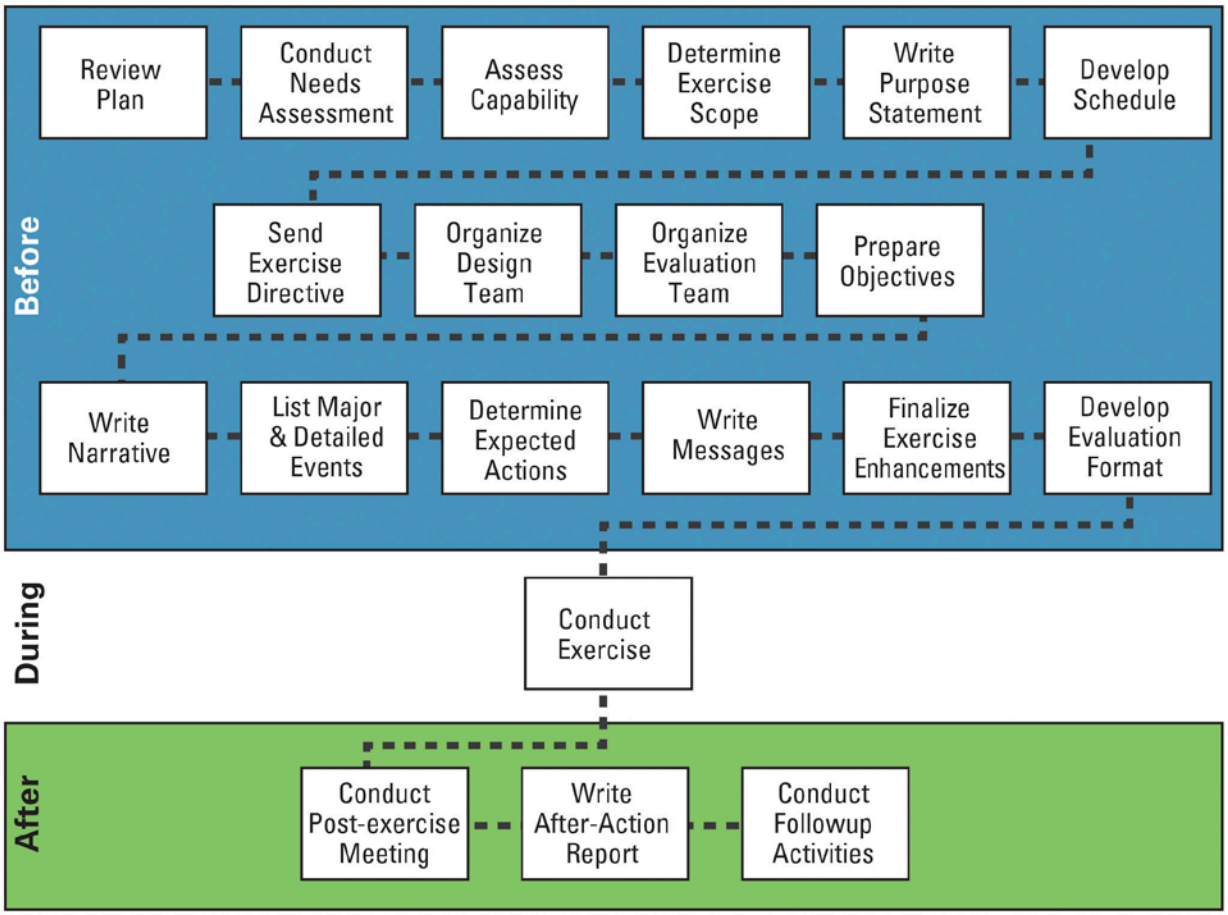


Figure 4: FEMA IS 139, Section 3 Exercise Process

An exercise strategy and schedule should address, at a minimum, the following:

A. Alignment of exercise objectives with BIAs. To ensure that your plans align with operational requirements, closely tie your exercise objectives with the requirements established by the BIAs. For example, if a service-level agreement requires a system to be available within 24 hours of an outage, exercises should include the 24-hour RTO.

B. Involvement of plan stakeholders throughout continuity planning and exercises. During an incident that requires continuity plan activation, communication with stakeholders is essential. The planning process should identify and engage key stakeholders and document their contact information. Before an exercise, those points of contact should be notified that you are conducting the evaluation, and exercise personnel should communicate to stakeholders information similar to what would be given during an actual event. This will ensure that points of contact are current; stakeholders familiar with the plan will help identify gaps in information needs across the organization.

C. Guidelines for tracking issues that arise during exercises. Expect differences between plans and outcomes of an exercise. Be prepared to capture those differences so that important gaps can be addressed

and plans can be updated. There are many possible strategies for addressing issues that arise during an exercise, such as interrupting your exercise for discussions or designating a recorder to document issues. Decide how to track and address issues, and ensure that the exercise has a way to capture that information.

D. Frequency and type of exercises. Establish a frequency for conducting exercises, and align this frequency with your organization's needs for ensuring that plans remain actionable.[20]

- **Frequency.** Services that are the most critical or experience considerable change may require more frequent and comprehensive testing.
  a. Annual testing is usually sufficient for most services.
  b. Quarterly or monthly testing may be appropriate for very critical services or those with a high rate of change.
  c. Timing of the exercise should consider the potential impact to the delivery of the service.
- **Type of exercise.** There are many approaches for conducting a continuity plan exercise. Typically service continuity plans are tested through a progression of exercises, from the simplest tabletop exercise to the most complex integrated plan testing.
  a. **Tabletop exercises.** Tabletop exercises are reviews of plans, policies, and procedures. They provide an opportunity for the recovery team to walk through the actions to be taken.
  b. **Partial-function recovery exercises.** Partial recovery exercises simulate a degraded operation and exercise the plan's ability to restore operations when only portions of the infrastructure and resources are available. Partial testing allows the service to stay online and presents minimal risk to the operation of the service.
  c. **Full-function recovery exercises.** Full-function exercises test recovery from the loss of an entire business service or IT system. This type of test may require complete recovery of the service at an alternate location and presents a risk of an impact on the business service if there are issues with the recovery plan.
  d. **Integrated recovery tests.** Integrated recovery testing identifies areas for improvement when multiple plans are activated together or when there are external dependencies for plan execution. Integrated testing is usually conducted with
     - exercises of other plans, such as for upstream and downstream services
     - external organizations and stakeholders

E. Exercise planning and documentation. Exercise templates or planning tools can help organizations comply with standards and provide consistent results for reporting.

See Appendix C for an example exercise template. An exercise process developed by the DHS National Protection and Programs Directorate and FEMA (http://www.ready.gov/business-continuity-planning-suite) can assist with exercise planning (http://www.ready.gov/business/testing/exercises).

i. The plan for conducting an exercise should include
   - the stakeholders involved in the exercise
   - exercise support staff, including a facilitator and recorder
   - role descriptions and expectations for each stakeholder
   - scenario to be used (proposed disruption particulars)
   - objectives of the exercise (what it should prove or disprove)
   - specific exercise activities to be performed
   - infrastructure requirements (information, technology, and facilities, as well as conditions necessary to perform the exercise)

- criteria for stopping the exercise
- back-out procedures to prevent service interruption if the exercise fails
- expected exercise results (including specific measures and targets for those measures such as availability requirements)
- documentation of the resolution or status of issues that may have been identified in previous exercises
- instructions for documenting and recording the results of the exercise for later review
- guidelines for developing a corrective action plan to address problems encountered
- scripts or procedures that outline the steps that will be taken to meet the objectives of the exercise

ii. Exercise plans should be reviewed by continuity plan owners and stakeholders.

Step 3. Exercise service continuity plans.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Reference
Goal 3: Service continuity plans are tested to ensure they meet their stated objectives.	
3. Are service continuity plans tested? [SC:SG5.SP3]	PR.IP-10: Response and recovery plans are tested.
4. Are backup and storage procedures for high-value information assets tested? [KIM:SG6.SP1]	PR.IP-4: Backups of information are conducted, maintained, and tested periodically.

To maintain the viability of the organization's service continuity program, the organization must conduct regular exercises of continuity plans, identify improvements, and update the plans.[21] Exercises should be designed to become iteratively more comprehensive and address a variety of different scenarios over time. A leading practice is to develop exercise standards and strategies specifically designed to promote plan process improvement and the introduction of scenarios that stretch the capabilities of the continuity process. Some examples of exercise enhancements to consider include

- combined business, technology, and incident management exercises
- integrated exercises of multiple plans, including upstream and downstream dependencies among plans
- facility-wide exercises
- exercises with external providers or vendors
- regional exercises that may include interactions with a number of external groups

Before conducting an exercise, ensure that all stakeholders have been notified of the exercise and, if possible, engage the stakeholders in participating in some or all aspects of the exercise, including exercise planning.

A. Initiate the exercise. Ensure that the exercise start time and date is documented, and notify all affected parties that the exercise has begun.

B. Monitor the exercise. The exercise should be monitored for progress against the recovery objectives, for issues that would require stopping the exercise, and for time. It is crucial to document the various activities, results, issues, and observations throughout the exercise.

C. Close the exercise. The exercise should be formally closed, and all stakeholders should be notified that the exercise has been completed.

D. Document the exercise results. Document the results of exercises as prescribed by your organization's standards for exercise evaluation.

Step 4. Evaluate exercise results.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Reference
Goal 3: Service continuity plans are tested to ensure they meet their stated objectives.	
5. Are test results compared with test objectives to identify needed improvements to service continuity plans? [SC:SG5.SP4]	PR.IP-10: Response and recovery plans are tested. RC.IM: Recovery planning and processes are improved by incorporating lessons learned into future activities.

The evaluation of exercise results provides an opportunity to improve both continuity plans and their exercise plans. Areas for improvement might include overlooked resources, weak procedures, missing technology capabilities, infrastructure requirements, plan logistics, personnel skill gaps, or the cost of executing the plan.

A. Compare the documented exercise results against the established exercise objectives.[22]

B. Record areas for which objectives could not be met. Establish accountability for resolution of identified issues as well as targeted resolution timelines.

C. Track issues to closure. Issues identified and corrected may warrant a follow-up exercise for validation.

D. Review and revise the plans. After plans are modified, it is important to replace older versions with the newer ones in the repository so that the most current version is available to recovery teams.

E. Report exercise results. Follow the standards developed in Section III for reporting exercise results. Exercise reports typically include

i. individual exercise results
   a. detailed results and executive overviews
   b. identified issues, responsibility, and targeted resolution time frame

ii. program exercise results, containing the percentage of
   a. continuity plans in compliance with their exercise schedule
   b. interdependent continuity plans that have or have not been jointly exercised
   c. continuity plans that have failed one or more exercise objectives
   d. high-priority services that were not successfully recovered during exercise
   e. action items resulting from exercises resolved within a targeted time frame

Step 5. Conduct an after-action review of plan activations and execution.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Reference
Goal 4: Service continuity plans are executed and reviewed.	
2. Is execution of service continuity plans reviewed? [SC:SG6.SP2]	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed. RC.IM: Recovery planning and processes are improved by incorporating lessons learned into future activities.

If an organization has activated or executed a service continuity plan in response to an incident, it should review the response and the issues that were addressed during the recovery process, to reveal strengths and areas for improvement.[23] Compare the actions taken to predefined procedures in the plan, and identify where procedures could be improved or redesigned to be more effective.

The following are examples of activities in a typical after-action review.

A. List all participants and stakeholders in the review and their role in the response and recovery process. Note any issues or opportunities for improvement.

B. Identify lessons learned.

i. Describe the disruption.

ii. Discuss response and recovery, for example,

a. recovery team response

1. time to convene the team
2. initial assessment of the service interruption
3. leadership decisions, including plan activation
4. any coordination or actions that may involve the organization's incident management team

b. communication, both internal and external

c. IT response and recovery, including the ability to meet recovery objectives

d. business operations response and recovery, including the ability to meet recovery objectives

e. impact of other supporting activities, such as facilities, security, or human resources response, including

1. safety of employees
   - evacuation procedures and relocation
   - injuries and response

f. performance of external dependencies

C. Identify what went well. Review the areas in which performance met planned expectations, and identify strengths.

D. Identify areas for improvement. Identify areas in which performance did not meet expectations, and identify the cause.

E. Identify corrective actions. Assign responsibility for making improvements, including a time frame and next steps.[24]

F. Track open items to closure. Issues identified and corrected may warrant a follow-up plan exercise to validate changes.

Step 6. Perform service continuity training.

All staff assigned to roles and responsibilities in the service continuity plan must be trained in the performance of those roles. Plan reviews, exercises, and lessons learned through exercise and activation evaluations provide excellent opportunities for training.

A. Plan reviews and tabletop exercises. Plan reviews and tabletop exercises facilitate a hands-on walk-through of each team member's roles and responsibilities. They are opportunities to uncover specific skill gaps and training needed prior to committing resources to a live recovery exercise.

B. Exercise and activation evaluations. Lessons learned from the exercising and activation of plans highlight opportunities for improvement in both the plan and skill level of the staff who must execute the plan.

C. Partial- and full-function recovery exercises. Partial- and full-function recovery exercises provide the most realistic and advanced training, but they may be the most costly and risky environment in which to train.

D. Organization's existing training program and capabilities. The organization's existing training program may include many skills necessary to execute a service continuity plan. Skills specific to continuity and recovery may be included as content of existing training or continuity-specific courses.

Output of Section V

	Output	Guidance
✓	Resource conflicts identified	List of resources with conflicts and type of conflict
✓	Conflict mitigations	List of conflict resolutions and risk dispositions
✓	Summary of plan review results	• Percentage of plans that do not meet availability requirements • Percentage of plans that do not meet standards and guidelines • Percentage of plans with one or more severe conflicts (such as a single point of failure) that have not been mitigated
✓	Management approval to place plan into service	• Business owner acceptance memo signed • IT acceptance memo signed
✓	Guidelines and standards for service continuity exercises	• Identification and responsibilities of plan owners • Identification and involvement of stakeholders • Exercise process, strategy, and management • Plan exercise schedule • Requirements for what information must be documented during and after a plan exercise • Measures for how the organization evaluates incident management plan performance
✓	Exercise plans	A plan developed using pre-established exercise criteria
✓	Plan exercise results	• Acceptable response times and process adherence in accordance with the plan • Acceptable targets and current percentage of continuity plans that have failed one or more exercise objectives
✓	Strategy for exercising and maintaining service continuity plans	Guidelines for plan exercising; using lessons learned to improve service continuity plans
✓	Validated plans	Confidence that service continuity plans are viable and that when activated will meet the RTOs for critical services
✓	After-action evaluation	• Procedures for evaluating plan execution and providing lessons learned • Strengths and weaknesses identified • Improvements to be made
✓	Training	Guidelines for conducting service continuity training

VI. Improve Service Continuity

Before You Begin

The following checklist summarizes the tasks you will need to complete and the information you will need to gather before you can begin improving service continuity plans.

	Input	Guidance
✓	Program objectives, policies, and standards	• Determine if the program is functioning as documented • Measure program outcomes against stated objectives • Determine if the level of disruption risk is acceptable • Identify needed changes in strategy, oversight, governance, and reporting
✓	Change criteria for continuity program and plans	• Scheduled plan reviews; service continuity plans must be reviewed during any major change to the organization and after the plan has been exercised • Plan exercise results • Post-incident analysis and after-action reporting review

Step 1. Review overall service continuity program effectiveness.

Ensuring that the service continuity program remains effective requires ongoing monitoring of risks, threats, plans, and the organization's objectives. For most organizations, service continuity takes time to fully implement, and the process is a journey requiring regular tuning. Organizations typically need to make a series of program adjustments to keep pace with normal changes in their organization and the threat landscape.

The service continuity oversight or steering group, described in Section III, is typically best suited to take an active role in managing the program, monitoring the need to make adjustments, and coordinating improvement activities. The oversight group's role may include

- establishing refined or updated program strategies and objectives; many do this annually
- providing new or refined standards for plans and exercises
- identifying gaps or weaknesses that must be addressed
- developing communications to stakeholders
- modifying or strengthening training and awareness requirements
- establishing budgets
- identifying and implementing new program methodologies

Step 2. Proactively identify conditions for revising service continuity plans.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Reference
Goal 4: Service continuity plans are executed and reviewed.	
3. Are improvements identified as result of executing service continuity plans? [SC:SG7.SP2]	RC.IM: Recovery planning and processes are improved by incorporating lessons learned into future activities.
	RC.IM-2: Recovery strategies are updated.

Service continuity plans should be reviewed and updated after exercises, on an established maintenance schedule, or as changes occur that would affect the execution of the plan, such as a reorganization of departments and responsibilities.[25] It is advisable to require that maintenance updates to a plan occur at least annually. A leading practice is to conduct regular reviews of the continuity program's overall effectiveness and weaknesses and address any improvements by updating program standards, objectives, or methodologies (see Step 1 above).

The following steps will facilitate ongoing plan maintenance:

A. Maintain the continuity plan. Maintenance typically accounts for
   i. scheduled plan reviews, usually performed annually
   ii. changes in a service's or asset's availability requirements
   iii. identification of new vulnerabilities, threats, and risks
   iv. product or service changes
   v. staff changes
   vi. relocation of facilities
   vii. significant technical infrastructure changes
   viii. changes in relationships with vendors and business associates
   ix. changes in or additions to regulatory or legal obligations

B. Review the results of plan validation activities and assess performance against objectives. Validation results typically include
   i. plan reviews
   ii. exercise results
   iii. after-action evaluations

C. Determine areas for improvement.[26]
   i. Weaknesses discovered during exercises
   ii. Lessons learned from plan execution

Step 3. Make improvements.

A. Schedule and assign responsibility for improvements.

B. Update the service continuity program processes and plans.[27]

C. Track open items to closure.

Output of Section VI

	Output	Guidance
✓	Updated program processes	• Updated program strategy, objectives, documentation, and procedures • Document process change objectives, timelines, and responsibilities
✓	Updated continuity plans	Approved plan changes
✓	Updated continuity plan inventory or database	A database, spreadsheet, or list showing the current plan's publication date and all subsequent versions; a copy of this list is frequently found at the beginning of continuity plans

VII. Conclusion

Service continuity management is a foundational component of effective cybersecurity. Risks from disruptions that are the result of natural or man-made events continue to grow, making service continuity an ever more essential component of an organization's risk management. The BIA gauges the impact of such events on the organization by evaluating the disruption of its critical services. Expanding reliance on technology and a general trend toward a more interconnected global landscape are clearly key challenges that must be addressed. Those challenges must be managed in conjunction with the growing complexity and frequency of cyber attacks and natural disasters.

The variety of documentation, standards, guidelines, and regulations developed to address business disruption risk is extensive, but there are just a few straightforward foundational activities that they all share such as establishing a program, planning, validating and exercising, and improving. This document is organized around those common foundational activities to provide a standard- and guideline-agnostic approach to managing business disruption risk. While standards can be useful in identifying more detailed *how-to* activities, the approach taken by this guide is to provide a clear outline of *what* should be done to effectively manage disruption risk and service continuity.

The following documents provide standards and methodologies for preparing for and managing business disruptions:

- DHS/FEMA Private Sector Preparedness Program (PS-Prep)—voluntary program, primarily serving as a resource for private and nonprofit entities interested in instituting a comprehensive business continuity management system. The program adopted the following three preparedness standards (http://www.fema.gov/about-ps-preptm):
  - ASIS International (PDF 1.2 MB)
  - British Standards Institution (BSI)
  - National Fire Protection Association (NFPA)
- DHS/FEMA Business Continuity Planning Suite (http://www.ready.gov/business-continuity-planning-suite)
- NIST Special Publication 800-34, Contingency Planning for Federal Information Systems
- More information about pandemic planning can be found at
  - http://www.who.int/influenza/preparedness/pandemic/en/
  - http://emilms.fema.gov/IS520/index.htm
- The *CERT Resilience Management Model (CERT-RMM)* [Caralli 2010] is the basis for the CRR and contains more in-depth guidance for establishing cybersecurity practices. The Service Continuity practice area provides detailed description of practices and goals associated with disruption risk management.

- DHS Cyber Resilience Review (CRR, http://www.dhs.gov/xlibrary/assets/pso-safeguarding-and-securing-cyberspace.pdf).

For more information about the Cyber Resilience Review, please email the Cyber Security Evaluation Program at CSE@hq.dhs.gov or visit the website of the Office of Cybersecurity and Communications at http://www.dhs.gov/office-cybersecurity-and-communications.

Appendix A. Example Business Impact Analysis Template

<Organization Name> Business Impact Analysis

Department / Function / Process: _____

Operational & Financial Impacts: _____

Timing / Duration	Operational Impacts	Financial Impacts

Timing: Identify point in time when interruption would have greater impact (e.g., season, end of month/quarter).

Duration: Identify the duration of the interruption or point in time when the operational and or financial impact(s) will occur:

< 1 hour

> 1–8 hours

> 8–24 hours

> 24–72 hours

> 72 hours

> 1 week

> 1 month

Considerations (customize for your business)

Operational impacts:

Lost sales and income:

Negative cash flow resulting from delayed sales or income:

Increased expenses (e.g., overtime labor, outsourcing, expediting costs):

Regulatory fines:

Contractual penalties or loss of contractual bonuses:

Customer dissatisfaction or defection:

Delay executing business plan or strategic initiative:

Appendix B. Example Service Continuity Plan Template

<Area/Unit Name> Continuity Plan

Date: _____ Name of person completing this form: _____

Executive Support

List the organization executives who had input to this document and endorse its development and applicability.

Name of Executive	Date	Signature

Service(s) Description

Explain/define the service in a manner that provides high-level understanding to personnel who must implement this plan.

Service Priority

Indicate the priority of the services.

Priority Level	***Service Restoration Time Objective***

Continuity Plan Activation Criteria

Describe conditions that must be met before this continuity plan can be executed.

Assignment of Responsibility

List employees who are responsible for developing and maintaining this plan.

Name of Employee	Date	Signature	Responsibility

Communication Channel(s)

Identify communications channels to be used to notify stakeholders in the event this plan is to be executed.

Service Owner(s)

List the business owner(s) responsible for this area/unit.

Name of Employee	Date	Signature	Role

Essential Roles and Alternates

Identify roles essential for restoring and executing the service, as well as primary and backup/alternate personnel.

Role	Primary Personnel	Alternative Personnel

Essential Information Assets

List the information assets essential to the service.

Information Asset Name	Description	Logical Location	Physical Location	Backup Strategy and Schedule

Essential Technology Assets

List the technology assets essential to the service.

Asset Name	Description	Physical Location	Backup Strategy/Location

Alternate Site(s)

Identify the location(s) for any applicable alternate processing site for the service.

Site Name	Physical Location

Security or Access Issues

Describe any known security or access issues important to accessing the alternate sites, or security considerations in case of plan activation outside of normal operating hours. Consider both physical and logical access.

Recovery Objectives

List the known recovery objectives for the service. Include regulatory requirements and business obligations, such as service-level agreement information.

Obligation Name	Reference/Section	Relevant Text	Date Recorded

Schedule for testing this plan
This plan will be tested <defined frequency>
The date of the last test was <YYYY/MM/DD>

Related Continuity Plans

Identify any continuity plans that are related to this plan.

Plan Name	Relationship

Laws, Regulations, and Rules

Identify any and list legal requirements that must be considered when performing continuity planning.

Law or Regulation	Relevant Section or Text

Plans of Action

List the conditions that have been identified through risk and vulnerability assessments, as well as response actions.

Fire	Instruct personnel to evacuate the immediate area. Locate available fire extinguishers if possible and contact fire department.

Key Documentation

Identify technical manuals, reference guides, and other supporting materials that may be necessary to restore service operations.

Title	Location

Recovery Sequence for the Service

List step-by-step instructions for recovering the service at the normal operating facility.

Step Number	Action	Role Responsible
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		

List step-by-step instructions for recovering the service at the alternate operating facility.

Step Number	Action	Role Responsible
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		

Key Contacts

List the key contact information essential to the service and this plan. Include the service owner as well as internal and external technical support.

Name	Role	Company Name	Phone	Phone 2
	Service owner			
	Internal technical support for information assets			
	Internal technical support for technology assets			
	External technical support for information assets			
	External technical support for technology assets			
	Hardware vendor			
	Primary software vendor			
	Fire company			
	Police			
	Alternate operating site contact			
	Electric utility POC			
	Telecommunications POC			
	Water utility POC			
	Executive management			
	Legal counsel			
	Internal resource for continuity plan execution			
	Internal resource for continuity plan execution			
	Internal resource for continuity plan execution			
	Stakeholder who requires notification of plan activation			
	Stakeholder who requires notification of plan activation			
	Stakeholder who requires notification of plan activation			
	Regulatory organizations that require notification if this plan is activated			
	Health-care providers who should be notified if this plan is activated			
	Other organizations that should be notified if this plan is activated			

Appendix C. Example Service Continuity Plan Exercise Template (FEMA IS 139-Unit 8)

Evaluator Checklist

Evaluator: _____ **Date:** _____ **Location:** _____

Objective No.:	**Function Being Evaluated:**

Objective:

Performance Criterion *[#]*

Points of Review:

Please answer the following: Y = Yes, N = No, NA = Not Applicable, NO = Not Observed

	Y	N	NA	NO
1.				
2.				
3.				
4.				

Comments:

Narrative Summary

Objective Number: _____ **Criterion Number:** _____

Evaluator: _____ **Location:** _____

Issue:

A specific statement of the problem, plan, or procedure that was observed.

_____
_____
_____
_____
_____
_____
_____

Discussion:

A discussion of the issue and its specific impact on operational capability.

_____
_____
_____
_____
_____
_____
_____
_____

Corrective Action Recommendation:

Recommended course(s) of action to improve performance or resolve the issue to improve operational capability.

_____
_____
_____
_____
_____
_____
_____
_____

Narrative Summary (Continued)

Office of Primary Responsibility:

The department, agency, or organization responsible for implementation of corrective actions.

Department, Agency, or Organization:
_____

Individual Responsible: _____

Title: _____ **Date Assigned:** ___ / ___ / ___ **Suspense Date:** ___ / ___ / ___

Key Event Response Form

Event No. _____ Scheduled Date/Time _____

Initially Input To _____ Actual Date/Time _____

Response Date/Time	Position Responding	Action Taken

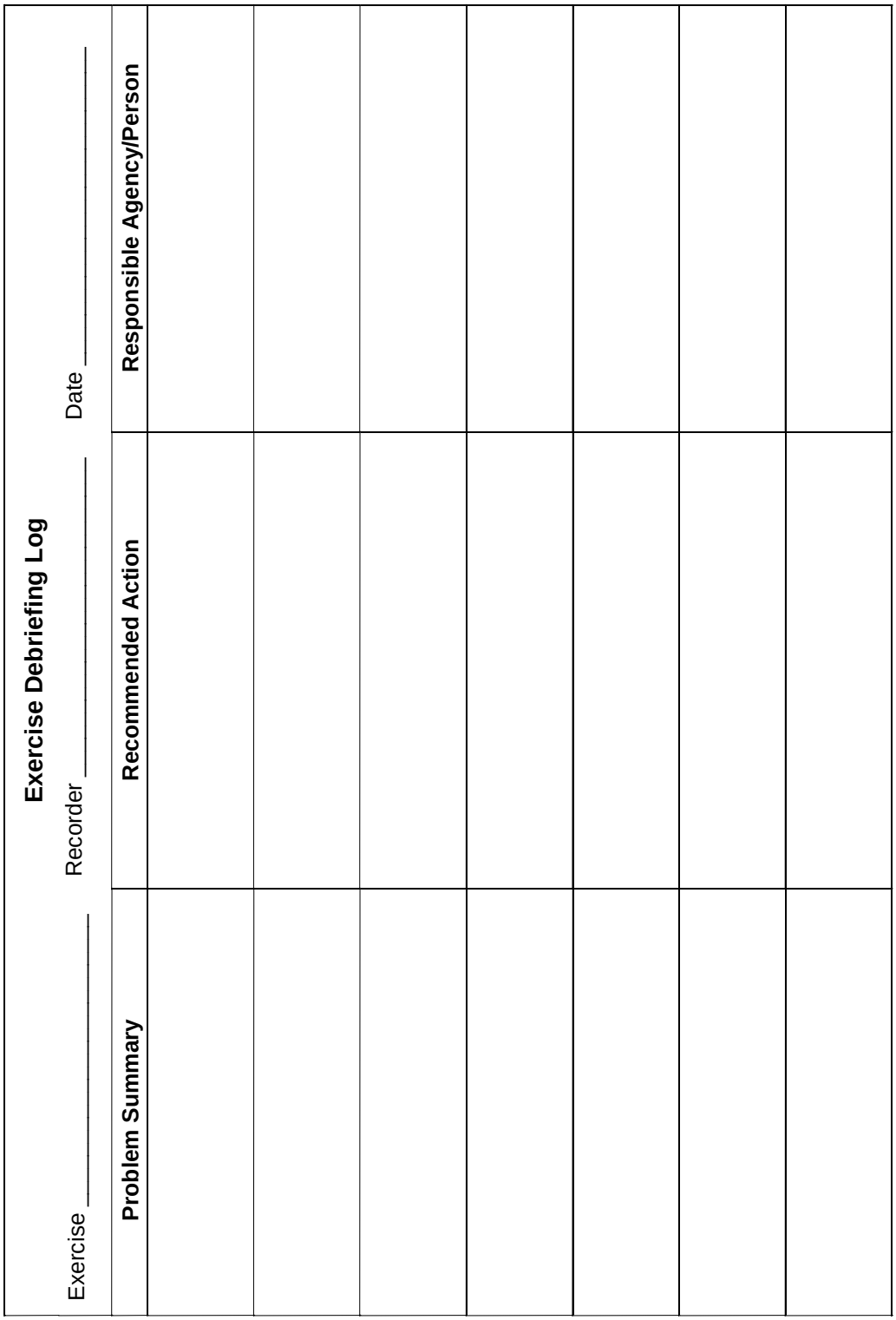
Problem Log

Date: _____

Exercise Assignment: _____ Tel. No: _____

Time	Message Library No. (if known)	Problem	Analysis (Leave Blank)

Exercise Debriefing Log



Appendix D. Service Continuity Resources

Association of Continuity Planners
http://www.acp-international.com/

- Association of Continuity Planners Chapters Map
  http://www.acp-international.com/index.php/chapters

Business Continuity Institute (Good Practice Guidelines and other resources)
http://www.thebci.org/

"Continuity Planning: Addressing Critical Business Processes That Support Implementation of HIPAA Transactions"
http://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/MMIS/downloads/continuity.pdf

Continuity Central
http://www.continuitycentral.com/

- Business Continuity Resources
  http://continuitycentral.com/resources.htm

Disaster Recovery Institute International
https://www.drii.org/

- Professional Practices for Business Continuity Planners and other resources
  https://www.drii.org/

Disaster Recovery Journal
http://www.drj.com/

- Generally Accepted Practices
  http://www.drj.com/GAP/GAP3.pdf

Federal Emergency Management Agency (FEMA)
http://www.fema.gov/

- PS-Prep—voluntary program, primarily serving as a resource for private and nonprofit entities interested in instituting a comprehensive business continuity management system. The program adopted the following three preparedness standards. For more information, see http://www.fema.gov/about-ps-preptm.
  - ASIS International (PDF 1.2 MB)
    http://www.fema.gov/redirect?url=http%3A%2F%2Fwww.asisonline.org%2Fguidelines%2FASIS_SPC.1-2009_Item_No._1842.pdf
  - British Standards Institution (BSI)
    http://www.fema.gov/redirect?url=http%3A%2F%2Fwww.bsiamerica.com%2Fen-us%2FAssessment-and-Certification-services%2FManagement-systems%2FStandards-and-schemes%2FBS-25999%2F

    - National Fire Protection Association (NFPA)
      http://www.fema.gov/redirect?url=http%3A%2F%2Fwww.nfpa.org%2Faboutthecodes%2FAboutTheCodes.asp%3FDocNum%3D1600%26cookie%255Ftest%3D1
- Business Continuity Planning (BCP) Suite
  http://www.ready.gov/business-continuity-planning-suite
    - BCP resources to assist businesses with preparedness
      http://www.ready.gov/business
- Exercise Design Materials
  http://www.training.fema.gov/emiweb/IS/is139lst.asp

Federal Financial Institutions Examination Council (FFIEC)
http://www.ffiec.gov/

- BC guidance Business Continuity Planning
  http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning.aspx

Gartner (requires subscription)
http://www.gartner.com/technology/home.jsp

- Best Practices for Conducting a Business Impact Analysis
  http://www.gartner.com/id=493210

Forrester
http://www.forrester.com/home/

- Business continuity articles, tools, and templates (some require a fee)
  http://www.forrester.com/search?tmtxt=Business%20Continuity%20%26%20Disaster%20Recovery&searchOption=10001&source=suggested

HIPAA.com
http://www.hippa.com/

- Continuity Plan: Disaster Recovery Plan–What to Do and How to Do It
  http://www.hipaa.com/2009/04/continuity-plan-disaster-recovery-plan-what-to-do-and-how-to-do-it/

International Organization for Standardization (ISO)
http://www.iso.org/iso/home.html

- 27002 Outlines potential cybersecurity controls and control mechanisms (fee)
  http://www.27000.org/iso-27002.htm
- The International Organization for Standardization (“Business continuity - ISO 22301 when things go seriously wrong”)
  http://www.iso.org/iso/home/news_index/news_archive/news.htm?refid=Ref1602
- ISO 27031:2011 Information Technology – Security techniques – Guidelines for information and communication technology readiness for business continuity (fee)
  http://www.iso.org/iso/catalogue_detail?csnumber=44374

National Institute of Standards and Technology (NIST)
http://www.nist.gov/index.html

- NIST Computer Security Division, Computer Security Resource Center
  http://csrc.nist.gov/
  - CMS Continuity Planning Tabletop Test Procedures
    http://csrc.nist.gov/groups/SMA/fasp/documents/continuity_planning/CP_Tabletop_Test_Template.doc
  - NIST Special Publication 800-30, Guide for Conducting Risk Assessments
    http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf
  - NIST Special Publication 800-34, Continuity Planning Guide for Federal Information Systems
    http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf
  - NIST Special Publication 800-66, An Introductory Resource Guide for Implementing the HIPAA Security Rule
    http://csrc.nist.gov/publications/nistpubs/800-66Rev1/SP 800-66-Revision1.pdf

SearchHealthIT
http://searchhealthit.techtarget.com/

- What Joplin teaches hospitals about disaster recovery planning
  http://searchhealthit.techtarget.com/tip/What-Joplin-teaches-hospitals-about-disaster-recovery-planning

Software Engineering Institute, CERT Division
http://www.sei.cmu.edu/

- CERT Resilience Management Model
  http://www.cert.org/resilience/rmm.html
- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)
  http://www.cert.org/octave/

Texas Health and Human Services Commission
http://www.hhsc.state.tx.us

- HHSC Disaster Recovery Plan Development Guide from the Texas HHS Commission
  http://www.hhsc.state.tx.us/contract/529130018/Procurement-Library/disaster-recovery-plan.doc

United States Computer Emergency Readiness Team (US-CERT)
http://www.us-cert.gov

- Situational awareness information
  https://www.us-cert.gov/

U.S. Department of Health and Human Services (HHS)
http://www.hhs.gov/

- Information Technology Continuity Plan Template
  http://www.hhs.gov/ocio/eplc/EPLC%20Archive%20Documents/36-Continuity-Disaster%20Recovery%20Plan/eplc_continuity_plan_template.doc

Appendix E. CRR/CERT-RMM Practice/NIST CSF Subcategory Reference

Table 2 cross-references CRR Service Continuity Domain goals and practice questions to the NIST CSF Categories/Subcategories and the sections of this guide that address those questions. Users of this guide may wish to review the CRR Question Set with Guidance available at https://www.us-cert.gov/ccubedvp for more information on interpreting practice questions. The NIST CSF, available at https://www.us-cert.gov/ccubedvp also provides informative references for interpreting Category and Subcategory statements.

Table 2: Cross-Reference of CRR Goals/Practices and NIST CSF Categories/Subcategories Against the Service Continuity Management (SCM) Resource Guide

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Reference	SCM Resource Guide Reference
Goal 1: Service continuity plans for high-value services are developed.		—
1. Are service continuity plans developed and documented for assets required for delivery of the critical service? [SC:SG3.SP2]	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.	Section III, Step 3 Section IV, Step 2
2. Are service continuity plans developed using established standards, guidelines, and templates? [SC:SG3.SP2]	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.	Section III, Step 2 Section IV, Step 2
3. Are staff members assigned to execute specific service continuity plans? [SC:SG3.SP3]	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed. RS.CO-1: Personnel know their roles and order of operations when a response is needed.	Section IV, Step 3
4. Are key contacts identified in the service continuity plans? [SC:SG2.SP2]	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed. RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams. RS.CO-4: Coordination with stakeholders occurs consistent with response plans.	Section IV, Step 2
5. Are service continuity plans stored in a controlled manner and available to all those who need to know? [SC:SG3.SP4]	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.	Section IV, Step 4
6. Are availability requirements such as recovery time objectives and recovery point objectives established? [TM:SG5.SP1]	ID.BE-5: Resilience requirements to support delivery of critical services are established. PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.	Section III, Step 3 Section IV, Step 2
Goal 2: Service continuity plans are reviewed to resolve conflicts between plans.		—
1. Are plans reviewed to identify and resolve conflicts? [SC:SG4.SP2]	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed. RC.IM: Recovery planning and processes are improved by incorporating lessons learned into future activities.	Section V, Step 1
Goal 3: Service continuity plans are tested to ensure they meet their stated objectives.		—
1. Have standards for testing service continuity plans been implemented? [SC:SG5.SP1]	PR.IP-10: Response and recovery plans are tested.	Section V, Step 2

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Reference	SCM Resource Guide Reference
2. Has a schedule for testing service continuity plans been established? [SC:SG5.SP1]	PR.IP-10: Response and recovery plans are tested.	Section V, Step 2
3. Are service continuity plans tested? [SC:SG5.SP3]	PR.IP-10: Response and recovery plans are tested.	Section V, Step 3
4. Are backup and storage procedures for high-value information assets tested? [KIM:SG6.SP1]	PR.IP-4: Backups of information are conducted, maintained, and tested periodically.	Section V, Step 3
5. Are test results compared with test objectives to identify needed improvements to service continuity plans? [SC:SG5.SP4]	PR.IP-10: Response and recovery plans are tested. RC.IM: Recovery planning and processes are improved by incorporating lessons learned into future activities.	Section V, Step 4
Goal 4: Service continuity plans are executed and reviewed.		—
1. Have conditions been identified that trigger the execution of the service continuity plan? [SC:SG6.SP1]	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed. RC.RP-1: Recovery plan is executed during or after an event.	Section IV, Step 5
2. Is execution of service continuity plans reviewed? [SC:SG6.SP2]	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed. RC.IM: Recovery planning and processes are improved by incorporating lessons learned into future activities.	Section V, Step 5
3. Are improvements identified as result of executing service continuity plans? [SC:SG7.SP2]	RC.IM-1: Recovery plans incorporate lessons learned. RC.IM-2: Recovery strategies are updated.	Section VI, Step 2

Endnotes

1. For more information on the *Cyber Resilience Review*, please email the Cyber Security Evaluation Program at CSE@hq.dhs.gov
2. The *CERT-RMM* (Glossary of Terms) [Caralli 2010]
3. Caralli, R. A.; Allen, J. A.; & White, D. W. *CERT® Resilience Management Model: A Maturity Model for Managing Operational Resilience (CERT-RMM, Version 1.1).* Addison-Wesley Professional, 2010. For more information on the CERT-RMM, please visit http://www.cert.org/resilience/rmm.html.
4. This document uses the term *exercise* instead of *test*, which has a pass/fail connotation.
5. "External Dependencies Management (EXT)," *CERT-RMM* [Caralli 2010].
6. The *CERT-RMM* (SC: SG3.SP2) [Caralli 2010] explains the need to document the key elements of the plan consistent with the standards and guidelines.
7. The *CERT-RMM* (IMC: SG4.SP1) [Caralli 2010] explains the need for incident escalation procedures, including escalation criteria.
8. The *CERT-RMM* (SC: SG3.SP2) [Caralli 2010] discusses developing plans for the delivery of a critical service.
9. The *CERT-RMM* (SC: SG3.SP2) [Caralli 2010] describes developing plans using established standards and guidelines.
10. The *CERT-RMM* (SC: SG2.SP2) [Caralli 2010] discusses identification of key contacts in service continuity plans.
11. The *CERT-RMM* (TM: SG5.SP1) [Caralli 2010] discusses the establishment of recovery time and recovery point objectives.
12. The *CERT-RMM* (SC: SG4.SP2) [Caralli 2010] discusses identification and resolution of plan conflicts.
13. The *CERT-RMM* (SC: SG3.SP3) [Caralli 2010] describes the assignment of staff to service continuity plans.
14. The *CERT-RMM* (SC: SG3.SP4) [Caralli 2010] discusses storage of service continuity plans.
15. The *CERT-RMM* (KIM: SG6.SP1) [Caralli 2010] discusses the testing of the organization's backup and storage procedures.
16. NIST Special Publication 800-53, Revision 3, "Recommended Security Controls for Federal Information Systems and Organizations"
17. The *CERT-RMM* (SC: SG6.SP1) [Caralli 2010] discusses the identification of triggers for the execution of service continuity plans.
18. The *CERT-RMM* (SC: SG5.SP1) [Caralli 2010] discusses the establishment of standards for testing service continuity plans.
19. NIST Special Publication 800-84, "Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities"

20. The *CERT-RMM* (SC: SG5.SP1) [Caralli 2010] discusses the establishment of a schedule for testing service continuity plans.
21. The *CERT-RMM* (SC: SG5.SP3) [Caralli 2010] discusses the testing of service continuity plans.
22. The *CERT-RMM* (SC: SG5.SP4) [Caralli 2010] describes the comparison of test results with objectives.
23. The *CERT-RMM* (SC: SG6.SP2) [Caralli 2010] discusses the review of service continuity plan execution.
24. The *CERT-RMM* (SC: SG7.SP2) [Caralli 2010] discusses improvements to service continuity plans following review of execution.
25. NIST Special Publication 800-34, "Contingency Planning for Federal Information Systems"
26. NIST Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations* [NIST 2010], covers the revision of the incident response plan to address system or organizational changes or problems encountered during plan implementation, execution, or testing.
27. The CERT Division's *Handbook for Computer Security Incident Response Teams (CSIRTs)* [West-Brown 2003] explains the need to validate the incident management policy as well as the importance of maintaining the policy as the organization changes.