CRR Supplemental Resource Guide
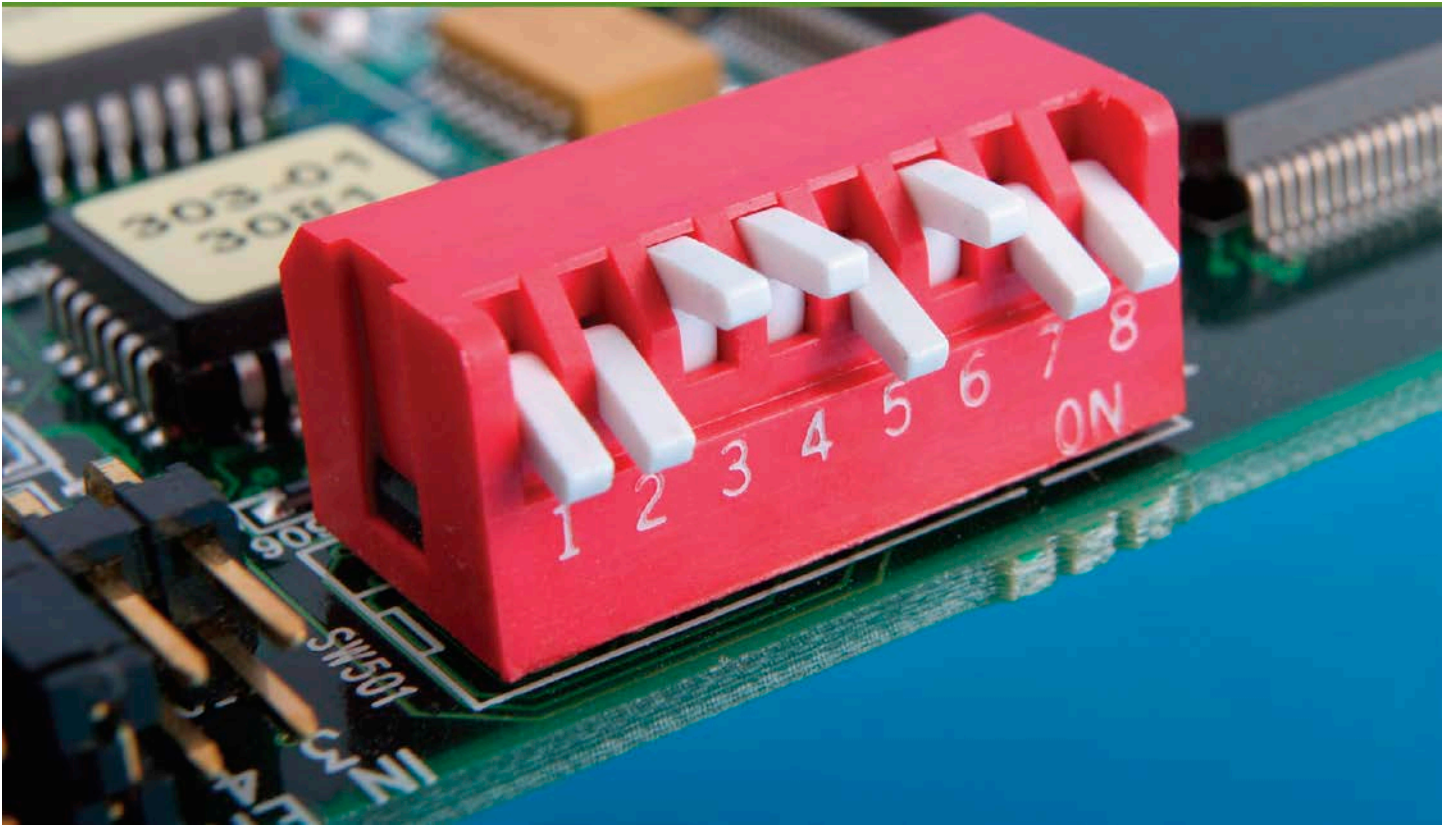
Volume 3

Configuration and Change Management

Version 1.1

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** ⇦*This guide*
4. Vulnerability Management
5. Incident Management
6. Service Continuity Management
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, assets identified in the Asset Management Resource Guide are often part of the configuration and change management plan.

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 configuration and change management process and for organizations seeking to improve their existing configuration and change management process. More specifically this guide
- educates readers about the configuration and change management process
- promotes a common understanding of the need for a configuration and change management process
- identifies and describes key practices for configuration and change management
- provides examples and guidance to organizations wishing to implement these practices

The guide is structured as follows:

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

II. Configuration and Change Management—Presents an overview of the configuration and change management process and establishes some basic terminology.

III. Create a Configuration and Change Management Plan—Details the process of creating a configuration and change management plan and identifies details that an organization should consider when developing its plan.

IV. Identify Configuration Items—Details the process of identifying assets that support critical services and will be configured and managed using this process.

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

Distribution Statement A: Approved for Public Release; Distribution is Unlimited

V. Implement and Control Configuration Changes—Details the process by which changes are approved, executed, and brought to closure.

VI. Monitor Configuration Changes—Details the process for assessing whether changes have occurred and procedures for addressing unauthorized changes.

VII. Conclusion—Summarizes the steps outlined in this document and suggests next steps for implementation.

Audience

The principal audience for this guide includes individuals who are responsible for designing, implementing, or overseeing configuration and change management in an organization. Senior executives who develop policies governing the implementation of configuration and change management may also benefit from this guide.

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

II. Configuration and Change Management

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
Goal 2: The integrity of technology and information assets is managed.	
1. Is configuration management performed for technology assets? [TM:SG4.SP2]	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained.

Overview

Configuration and change management (CCM) is the process of maintaining the integrity of hardware, software, firmware, and documentation related to the configuration and change management process. CCM is a continuous process of controlling and approving changes to information or technology assets or related infrastructure that support the critical services of an organization. This process includes the addition of new assets, changes to assets, and the elimination of assets.

> *The purpose of configuration and change management is to "establish processes to ensure the integrity of assets, using change control and change control audits" (CRR).*

As the complexity of information systems increases, the complexity of the processes used to create these systems also increases, as does the probability of accidental errors in configuration. The impact of these errors puts data and systems that may be critical to business operations at significant risk of failure that could cause the organization to lose business, suffer damage to its reputation, or close completely. Having a CCM process to protect against these risks is vital to the overall security posture of the organization. Figure 1 summarizes the four phases of the CCM process.
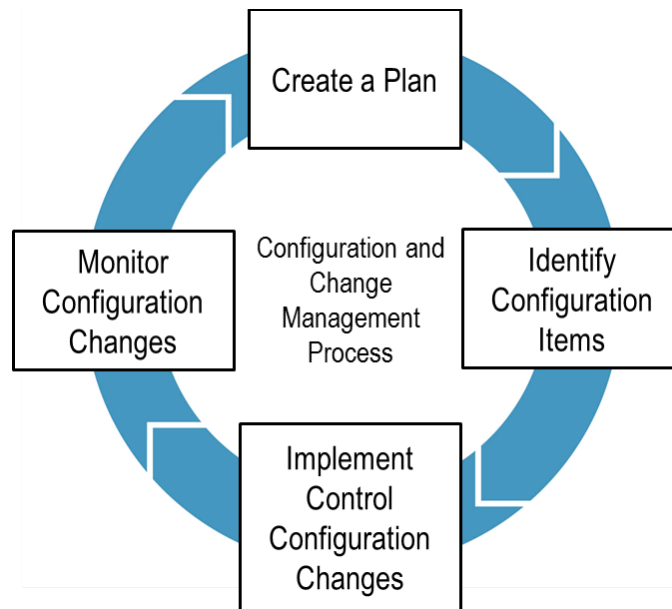
Figure 1: The Configuration and Change Management Process

Configuration and Change Management Terms

The following terms are associated with the CCM process:
- configuration item (CI)—an asset or series of related assets (typically focused on information or technology) that is placed under configuration management
- baseline configuration—a representation of the settings, software, and state of a CI, that is formally reviewed and agreed to at a given point in time and can only be modified through a formal CCM process. The baseline is used as a reference to manage the integrity of a CI over its lifecycle.[4]
- configuration and change management plan (CCMP)—the process by which changes to CIs are governed and implementation is executed. This includes policies and processes to request, approve, reject, implement, monitor, and improve changes to CIs.
- configuration management database (CMDB)—a database used to store configuration records throughout their lifecycle. A configuration management system maintains one or more configuration databases, and each database stores attributes of CIs and their relationships with other CIs.[4]
- configuration control review board (CCRB)—an organizational construct, made up of stakeholders, that is responsible for supporting the assessment, prioritization, authorization, and scheduling of changes to CIs and the implementation of policies governing those changes. ITIL refers to this construct as a Change Advisory Board.[4]

Configuration and Change Management Process

Create a Configuration and Change Management Plan

CCM enables the organization to control frequent changes to its high-value assets so that disruptions are mitigated and benefits are optimized. Resilient organizations are able to adapt to or roll back from changes that do not occur exactly as planned. For CCM, as with many activities, planning greatly impacts the success or failure of a project.

The following are the core foundational activities in planning for CCM:
- Obtain support for configuration and change management planning.
- Budget for configuration and change management.
- Define roles and responsibilities.
- Gather existing policies, procedures, and documentation related to configuration and change management.
- Identify critical organizational services that will require change and configuration management.
- Validate critical services with stakeholders and establish a configuration change review board.
- Develop a change request process.
- Determine how changes will be communicated to the organization.
- Develop a configuration and change management training plan.
- Identify tools for use in implementing and monitoring configurations.
- Plan for capacity management.

Identify Configuration Items

A configuration item is any system component, infrastructure component, document, or other item that needs to be managed to control the introduction of errors into the critical system or service.

The following are the core foundational activities in identifying CIs:
- Map critical organizational services to stakeholders and related services.
- Identify assets related to the critical services.
- Identify the CIs of the assets that will undergo change and require change and configuration management.
- Determine a configuration baseline for each CI.

Implement and Control Configuration Changes

Once all of the CIs have been identified and the most current configuration baseline has been tested and approved, changes can be applied to the systems. Baseline configurations are modified to maintain compliance with internal and external requirements and organizational goals. For a typical information technology system, the baseline should address installed software, patch levels, security posture, and system function. Where possible, the use of automated tools to apply the configurations is recommended. This lowers the risk of incorrectly applying configurations and provides an audit trail of the steps taken.

The following are the core foundational activities in implementing configurations:
- Evaluate change requests and approvals.
- Model configuration changes in a test environment.
- Deploy changes in the production environment.
- Determine the success or failure of changes.
- Roll back unsuccessful changes.
- Close out completed changes.
- Change configuration baselines.

Monitor Configuration Changes

Controlling the changes to the baseline configurations of ever-evolving systems represents a major challenge to organizations. In this phase, organizations ensure that changes are identified, proposed, reviewed, and tested prior to implementation.

The following are the core foundational activities in monitoring configuration change:

- Identify systems or components not specified in documentation.
- Identify disparities between authorized, approved baselines and actual, implemented baselines.
- Monitor system logs for unauthorized changes.
- Collect existing audits and configuration control records.
- Define remediation action.
- Execute monitoring plan.

III. Create a Configuration and Change Management Plan

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
Goal 1: The lifecycle of assets is managed.	
1. Is a change management process used to manage modifications to assets [ADM:SG3.SP2]	PR.IP-3: Configuration change control processes are in place.

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 CCM plan.

	Input	Guidance
✓	Scoping statement	This statement defines what needs to be addressed by the CCM plan. The plan should cover, at a minimum, all critical organizational services. Organizations that are not sure where to start should focus on the most critical services that affect their mission. If your organization has participated in a CRR, it may be beneficial to begin with the critical services addressed during the CRR.
✓	List of stakeholders	The list of stakeholders should be aligned to the scoping statement and include all appropriate internal and external entities. Potential stakeholders include • executive and senior management • heads of business lines, especially critical service owners • relevant internal business units: information technology, human resources, legal • external stakeholders—key customers or consumers of critical services • third-party providers (e.g., off-site hosting services)
✓	Approval of approach to CCM	• Approval from management for the intended approach to CCM, including stakeholder expectations about acceptable risk tolerance for the identified critical assets and services
✓	Externally imposed requirements for CCM	• CCM requirements defined by regulations and external needs • Changes required to meet service-level agreement requirements for critical services that are provided to external entities
✓	Budget for CCM	Identification of available funds to perform CCM planning and execution including • staffing resources • CCM software/hardware • third-party support
✓	Assignment of CCM roles and responsibilities	• Job descriptions for roles that have responsibilities for CCM planning, development, and delivery and that have executive ownership of CCM
✓	Risks	• A list of categorized and prioritized risks. As risks change over time, the list must be updated and made available. Any new risks may require modification of the CCM plan, so identifying new risks is critical.

Step 1. Obtain support for configuration and change management planning.

Management support is essential for an effective CCM plan (CCMP). Senior executive (C-level) support is often necessary for a CCMP being developed for an entire organization. For plans scoped to an individual service, only sponsorship from senior management responsible for the service may be necessary. For example, consider a hospital that has the following departments: Emergency Room, Cardiology, Radiology, Laboratory, Pharmacy, Surgical Services, Orthopedics, Physical Therapy, Information Services, and Materials Management. Configuration changes may affect each of these critical business functions differently, and large-scale changes could impact them all. Senior management needs to balance the responsiveness of CCM managed at each individual unit against the cost savings that can be achieved by managing it at a higher level.

Step 2. Budget for configuration and change management.

As part of obtaining initial support for a CCMP, the organization should allocate a budget for ongoing planning, execution, monitoring, and improvement of CCMP activities. This budget should include line items for the following:

- people resources (staff effort, outside consulting, and contracting)
- purchasing and supporting automated tools (hardware and software)
- creating and maintaining a modeling and testing environment (described in Section V)
- training staff who will be executing the change
- consulting services and contractors to help implement configuration changes
- training for users of updated CIs
- contingency funds for emergency change execution and management

Step 3. Define roles and responsibilities.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
Goal 1: The lifecycle of assets is managed.	
3. Is capacity management and planning performed for assets? [TM:SG5.SP3]	PR.DS-4: Adequate capacity to ensure availability is maintained.
Goal 2: The integrity of technology and information assets is managed.	
4. Are integrity requirements used to determine which staff members are authorized to modify information assets? [KIM:SG5:SP1]	PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties.
	PR.IP-3: Configuration change control processes are in place.
	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening).
8. Has a process for managing access to technology assets been implemented? [TM:SG4.SP1]	PR.AC: Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.

Table 1 defines typical CCMP roles and responsibilities. The roles and responsibilities defined here do not include other roles and responsibilities that the organization defines and may assign to an individual. For example, the configuration manager may also be the human resources manager. The CCM software that the organization selects may label the roles and describe their responsibilities differently.

Table 1: Typical CCMP Roles and Responsibilities

Role	Responsibilities
Chief Information Officer (CIO)	Responsible for setting change management (CM) policies and implementing CM at the highest level for the organization.

System Owner/Manager	Responsible for developing functional requirements and verifying that the requirements are implemented appropriately. This individual may also play a role in establishing and selecting members for the configuration control review board (CCRB). System owners and managers also fulfill the following roles in the execution of configuration changes: • CI owner • configuration baseline owner • configuration implementation owner
Configuration Manager	Oversees all aspects of the CCMP. The configuration manager is responsible for all day-to-day activities necessary to support the CMMP and may call on other personnel for assistance.
Configuration Control Review Board	The governing body for CCM policy and guidance affecting the organization. The CCRB should appoint a chairperson to oversee the activities of the board.
Information System Administrators	Help develop configuration baselines, impact analysis, and monitoring activities and are also responsible for complying with the CCMP for implementing changes to systems.
Information System Users	Responsible for reporting any weaknesses that are identified in current versions of the hardware, software, and components. Users initiate change requests, assist in testing baselines, and comply with the CCMP.
Configuration and Change Management Auditor	Responsible for auditing and reporting all phases of the CCM. Provides reporting to CIO, system owners, configuration manager, and CCRB.

While defining roles and responsibilities, access policies for configuration changes to CIs must be defined and included. These should be developed using the resiliency requirements for the services that each CI supports. Organizations should also consider the principles of least privilege and separation of duties when developing access policies. When determining who needs access to be able to modify information and technology assets, always consider how an individual's access might affect the asset's integrity. The goal is to ensure that the following qualities of the information remain unchanged:
- complete and intact
- accurate and valid
- authorized and official

Access to CIs can be controlled using two primary methods:
- physical—includes limiting physical access to computer rooms, file rooms, work areas, and facilities
- electronic—includes applying access control lists (ACLs) to networks, servers, applications, databases, and files

Access to CIs should be monitored closely, and the organization's internal regulatory divisions should address any deviations from the expected access. Section VI details the monitoring of CIs.

Step 4. Gather existing policies, procedures, and documentation related to configuration and change management.

Existing documentation will provide insight into the organization's unique requirements for implementing changes. It will also help identify any relevant external requirements, including regulatory boards or entities that must be considered in the design and implementation of changes. Also gather information collected as part of any other CRR implementations to reference when developing a CCMP.

Step 5. Identify and prioritize critical organizational services that will require change and configuration management.

Compile a list of the critical organizational services and the various CIs essential to each service. This is performed as part of an organization's asset management activities (see the Asset Management Resource Guide, Volume 1 of this series). The relative priority of the CIs and related services should receive special

attention. Often, organizations do not have the resources available to address all of the concerns immediately. Prioritization will allow an organization to address high priorities first and schedule lower priority areas to be addressed later. Some considerations for determining critical business functions are the following:

- What business objective does the service support?
- Do other services depend on this service to complete their tasks?
- What is the cost of disruption if the service fails?
- What is the potential punishment (e.g., fines, litigation) for failure of the service?
- Is there a potential for revenue or reputation loss?
- Who is responsible for service (list the person, role, or group)?

Once all of the critical services have been identified and prioritized, record all information in a chart. This chart could be in the form of a business impact analysis.

Step 6. Validate critical services with stakeholders and establish a configuration change review board.

Meet with stakeholders to validate the identified critical services and add any other critical CIs that may not have been identified. It is important to include stakeholders external to the organization in this process. External entities may also support the CCMP, so they may be part of the approval process for a particular change. Internal entities that may be involved include

- executive sponsor(s) of the CCMP
- senior leadership that can provide authority to enact changes
- heads of critical business units
- leads of the organization's functional departments responsible for enacting configuration changes (IT, facilities, HR)
- information system owners and administrators
- service owners
- end users of the service internal to the organization

This step results in the establishment of a configuration change review board (CCRB) responsible for reviewing, approving, and evaluating the efficacy of changes. The organization should develop a charter that gives this group the formal authority to approve and deny changes. This group is also responsible for the approval of any changes to the baseline configuration of any CIs. Section V discusses this in greater detail.

Step 7. Develop a change request process.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
Goal 1: The lifecycle of assets is managed.	
2. Are resilience requirements evaluated as a result of changes to assets? [RRM:SG1.SP3]	PR.IP-3: Configuration change control processes are in place.

The CCRB should develop and implement a process for individuals to request changes to CIs. (Appendix A includes an example of a change request form.) Typically, change requests are routed to a designated change manager, who will then complete the following activities in support of the CCRB:

1. Gather these requests and periodically review them with the CCRB.
2. Gather information from stakeholders about impacts of the change.
   o When changes would cause a large impact on the organization, obtain approval and scheduling guidance from the CCRB and senior leadership.

3. Communicate
   o approved changes to the change owner for implementation
   o denied changes, with an explanation, back to the change requestor

It is important to consider how changes to assets might also affect the resilience requirements of those assets. Before deciding whether to modify assets that affect critical services, the CCRB should be made aware of each asset's resilience requirements. The change request should also include this information, which the critical service owner(s) should review as part of the change impact analysis.

Step 8. Determine how changes will be communicated to the organization.

Create a communications plan that details how change notifications will be delivered. The communications plan should tailor the periodicity and type of information to the needs of each stakeholder. The scope, impact, and risks of any configuration change will also determine the level of communication detail required.

Step 9. Develop a configuration and change management training plan.

Implementing a CCMP usually entails a change in the fundamental culture of an organization. Determining if there are gaps in the staff's relevant knowledge, skills, and abilities and if the organization has appropriate training will greatly impact the success of the plan. It is also important for an organization to determine if it has staff qualified to enact the needed changes. Training those responsible for evaluating, approving, initiating, and monitoring changes is necessary to reduce the probability of executing unsuccessful changes. It may be beneficial to create a skills matrix for each role involved in the configuration and change process and compare it against any existing skills inventories. This will help identify gaps and suggest areas where training should be offered or additional staff may need to be hired. End users of the changed CIs and other stakeholders may also require training on any new usage patterns and workflows.

See the Training and Awareness Resource Guide, Volume 9 of this series.

Step 10. Identify tools for use in implementing and monitoring configurations.

There are various tools for managing the general CCM process. These tools track the overall process of configuration changes, including requests, status, communications, and issues related to changes. An organization should select a tool that meets its particular needs. Configuration information, including configuration baselines and historical changes to baselines and assets, is often consolidated in a configuration management database tool. There are also software tools, such as versioning repositories, that help manage changes in documentation. The CIs subject to the configuration management process, and their associated software, will often determine the choice of tools. Automated facility management tools that control electrical and HVAC resources can configure and monitor facilities assets. Various software packages can update engineering diagrams and other information assets, though licensed professionals should be involved in the updating of building engineering documents. Other tools can track skills inventories of people assets and give an overall view of training levels across an organization. The choice of tools also depends on the budget that is available for implementing configuration management.

Step 11. Plan for capacity management.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
Goal 1: The lifecycle of assets is managed.	
3. Is capacity management and planning performed for assets? [TM:SG5.SP3]	PR.DS-4: Adequate capacity to ensure availability is maintained.

Capacity planning and management is closely tied to CCM, but it is normally performed outside of the CCMP process. Capacity planning should lead to the specification of resilience requirements, which will impact the CCMP. The factors that determine an organization's capacity needs over time are dependent on the organization's business needs and growth. Some factors that should be considered when creating a capacity management plan include

- current utilization, whose analysis and metrics can be used to help plan any increase
- anticipated organizational growth or contraction as from mergers or spin-offs of organizational entities
- current and historical people, information, technology, and facility projections

Table 2 outlines some of the factors to consider when performing capacity planning:

Table 2: Capacity Planning Factors per Asset Type

People	Information	Technology	Facilities
• resources currently supporting critical services • supporting external resources	• size of databases for documentation of critical services • size and utilization of internal and external contact databases	• computational capacity • memory capacity • disk storage • network bandwidth (internal/external) • software licenses • user access licenses	• electricity (available amperage) • cooling (BTU) • physical storage space • staff workspace • meeting workspace

Output of Section III

	Output	Guidance
✓	Scope of the CCMP	This defines the overall goals of the plan and addresses the organization's current concerns and areas of greatest need. Knowing the scope of the plan allows an organization to implement the CCMP in a phased approach to address the most critical areas first. If your organization has participated in a CRR, it may be beneficial to reference the results. See Appendix D for a cross reference between the CRR and the steps in this guide.

✓	Budget for CCM	Available funding to support the CCMP process, to include
		• human resources (staff, contractors, consulting)
		• tools used to enact change
		  o CM databases and other CM tools
		  o development of custom tools
		  o consulting fees for tool implementation
		• contingency funding for emergency or unplanned changes

✓	Formal charter for CCRB	This document outlines the role of the CCRB and includes a statement of support by senior leadership that gives the CCRB the authority to enact and manage configuration changes in the organization, even in emergency situations.
✓	List of critical services	This list is essential to properly defining the CIs.
✓	Matrix of roles and responsibilities for CCMP	Defines the following roles in detail: • change manager • change owner • system owners

✓	List of stakeholders	Defines the following stakeholder groups:
		• external
		  o customers
		  o external suppliers (contractors, tool vendors)
		  o regulatory boards and agencies
		• internal
		  o senior management
		  o human resources department
		  o compliance personnel (internal audit, information assurance team)
		  o service owners
		  o users
		  o nonuser staff
		  o system/application owners

✓	Capacity Management Plan	Requests for increases in capacity will feed into the CCMP process. The capacity management plan is developed outside the change management process and should include • capacity forecasts for assets • statistics and metrics that will be used to measure capacity and performance Changes in configuration may positively or adversely impact future capacity management plans.

Distribution Statement A: Approved for Public Release; Distribution is Unlimited

IV. Identify Configuration Items

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 identifying CIs.

	Input	Guidance
✓	List of critical organizational services	Identifying critical organizational services will determine which systems must be subjected to the configuration management process. Some considerations for determining critical business functions are the following: • What business objective does the service support? • Do other functions depend on this function to complete their tasks? • What is the cost of disruption if the function fails? • What is the potential punishment (e.g., fines, litigation) for failure of the function? • Is there a potential for revenue or reputation loss? • Who is responsible for the function (list the person, role, or group)?
✓	Resilience requirements for critical services	The resilience requirements for services will determine the requirements for the associated assets that become CIs. These should be documented when the CI is identified.

It is crucial to produce an accurate listing of all systems that require CCM. It is at this level that each CI's baseline configuration is developed, reviewed, and approved. Recall that CIs are assets or series of related assets (typically information or technology focused) that are placed under configuration management. The configuration baseline serves as the basis for further activity for the CI and can be changed only through the formal process of change management. Also in this step, the organization determines the impact that a failure or loss of a CI would have on the critical services. Identifying if the CI has a high, medium, or low impact on the organization will determine what level of CCM the CI will be subject to. Identifying assets that do not require CCM is also important at this stage.

Step 1. Map critical organizational services to stakeholders and related services.

In this step, critical organizational services are associated with stakeholders and other related services. To illustrate, consider the example of an online retail site. The website must be available for browsing, the shopping cart must be available for customer checkout, the forms for customer input must be available, and the order must be able to be placed. These services all depend on each other, and a loss of any of these functions could cost the business a loss of revenue and potentially of reputation. The criticality of these services would be considered high. Table 3 maps these services to the person or team responsible, impacted stakeholders, and impacted services.

Table 3: Example Mapping of Critical Services

Service	Criticality	Person/Team Responsible	Impacted Stakeholders	Impacted Services
Site catalog	High	Web Team	Customers	Order processing
Shopping cart	High	Web Team	Customers, accounting	Order processing
Checkout	High	Accounting	Customers, accounting, supply chain	Order processing, accounts receivable, inventory management
Customer information input	High	Customer Relations	Customers, external governing bodies	Order processing, shipping

Step 2. Identify assets related to the critical services.

Once all of the critical services have been identified and mapped to stakeholders, the organization should identify the assets that those services use. The assets may include the following:

- servers
- storage arrays
- networking equipment and infrastructure (including cable and fiber runs)
- applications
- databases
- facilities (data centers, Independent Distribution Frame [IDF] and Main Distribution Frame [MDF] closets)
- power and cooling equipment (generators, uninterrupted power supplies, Automatic Transfer Switch [ATS])
- documentation

The criticality of each asset is determined by the highest criticality of any of the services that it supports. For example, if an asset supports both high- and medium-criticality business functions, it will receive a criticality of high. Consider a server that is used as a hypervisor for a virtual environment. The server may host many servers and workstations. If one of the them is running a system with a high criticality, the entire hypervisor will have a high criticality. If the hypervisor fails, then the virtual machine supporting the service will also fail.

Step 3. Identify the configuration items of the assets that will undergo change and require change and configuration management.

Each asset should be broken down into the components that will require configuration and change management. These are the CIs that will be managed. CIs can be one or a combination of the following:

- hardware
- software
- firmware
- facilities
- documentation (e.g., process documentation and service-level agreements)

Like assets, each CI will receive the same criticality designation of the highest criticality system and business service it supports. Each CI should be assigned a unique identifier so that it can be tracked through the service lifecycle. The following is a partial list of attributes to track for the item:

- unique identifier

Distribution Statement A: Approved for Public Release; Distribution is Unlimited

- item type (e.g., hardware, software, firmware, documentation)
- system name
- system purpose
- system owner
- make
- model
- serial number
- location

Step 4. Determine a configuration baseline for each configuration item.

Each CI will have a configuration baseline. The configuration baseline is the agreed-to description of the state of a CI's attributes, and it will serve as the basis for change management. Most baselines are established at a fixed point in time. The baseline should include the patch level, firmware version, and document release version. The following is a list of attributes that, at a minimum, should be collected about the CI.

- CI unique identifier
- patch level or document release version
- firmware version
- software version
- last approved configuration change
- related CIs

Output of Section IV

	Output	Guidance
✓	List of critical organizational services	Determines what services must be protected. This could be a business impact analysis for organizational services.
✓	Functions or services mapped to stakeholders	Mapping functions or services to stakeholders will give perspective on who data owners are.
✓	Systems related to critical services are identified	Will determine what level of configuration and change management must be applied.
✓	CIs that need configuration and change management are identified	Once all systems are broken into individual CIs, the items can be tracked within the CCMP.
✓	Configuration baselines	An agreed-to description of the attributes required for the baseline of a CI.

V. Implement and Control Configuration Changes

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 implementing configuration changes.

	Input	Guidance
✓	Configuration baselines for CIs	The baseline configurations for each CI will be the starting point for any configuration activity.
✓	Modeling and testing environment	An environment should be in place to allow for testing of configuration changes prior to deployment. This environment should mirror the production environment as closely as possible given financial and other resource constraints.
✓	Matrix of roles and responsibilities	List of individuals responsible for evaluating, testing, and implementing changes. • Only individuals with a need should have access to CIs. • Use physical means (e.g., room access, locked cabinets) and logical means (e.g., ACLs, firewall rules) for controlling access. • Access levels should be documented and changes to access should be approved by system owners and primary stakeholders. • These are addressed in detail in Section III.

Use automated tools whenever possible to perform configuration changes.

To maintain consistency when performing any type of configuration change, use automated tools and systems wherever possible. This will help ensure changes are applied uniformly across CIs and allow for automated rollback of any changes that are not successful. There are many tools available that can perform these tasks, but the better tools have these features:
- tight integration with a configuration management database (CMDB)
- work on multiple platforms (Windows, Linux, HP-UX, OSX)
- support applications and documentation in addition to operating systems and hypervisors
- automatically scan existing configurations and compare them against the current baseline and against requirements from external regulators (e.g., Protected Critical Infrastructure Information program, Defense Information Systems Agency)
- granular security and access controls that integrate into the existing authentication environment and auditing systems

When a single tool is not available to address all needs, verify that multiple tools are compatible and can all tie into the CMDB.

Distribution Statement A: Approved for Public Release; Distribution is Unlimited

Step 1. Evaluate change requests and approvals.

Any formally requested configuration change should go through a process of evaluating change requests and impact assessment as illustrated in Figure 2.

1. All change requests should be entered in a standard format (see Appendix A for an example of a change management request form).
2. When a new configuration change is requested, key stakeholders should analyze the impact of this change PRIOR to the meeting of the CCRB (see Appendix B for an example of an change impact analysis template). The analysis results must be available to the CCRB when they evaluate the requested change.
3. Some routine changes may not require CCRB approval. For example, the process for adding new users may be well defined and documented, and the submission and tracking of required documentation may be all that the CCRB requires. The CCRB should provide guidance on what may fall into this category.
4. Change requests should then be presented to the CCRB to be assessed for the following aspects:
    o benefits to the critical service supported
    o appropriateness of change management at CCRB level (small changes that do not impact the critical service might be managed at a lower level)
    o resilience requirements of the organization and how this change will impact those requirements
    o financial implications
    o potential risks of performing or not performing the change
    o impacts to resilience requirements of the CIs and related assets
    o urgency
    o change manager
    o system or application users who should be involved with the technical evaluation of the request

5. Once the CCRB approves the change, the change manager should evaluate the request and the system or application owners should assess the technical implications. Aspects to consider include
    o impacts to connected systems
    o impacts to users and usability
    o impacts to non-IT systems
    o training or technical expertise required to enact the change
    o scheduling considerations to minimize any disruptions caused by the change
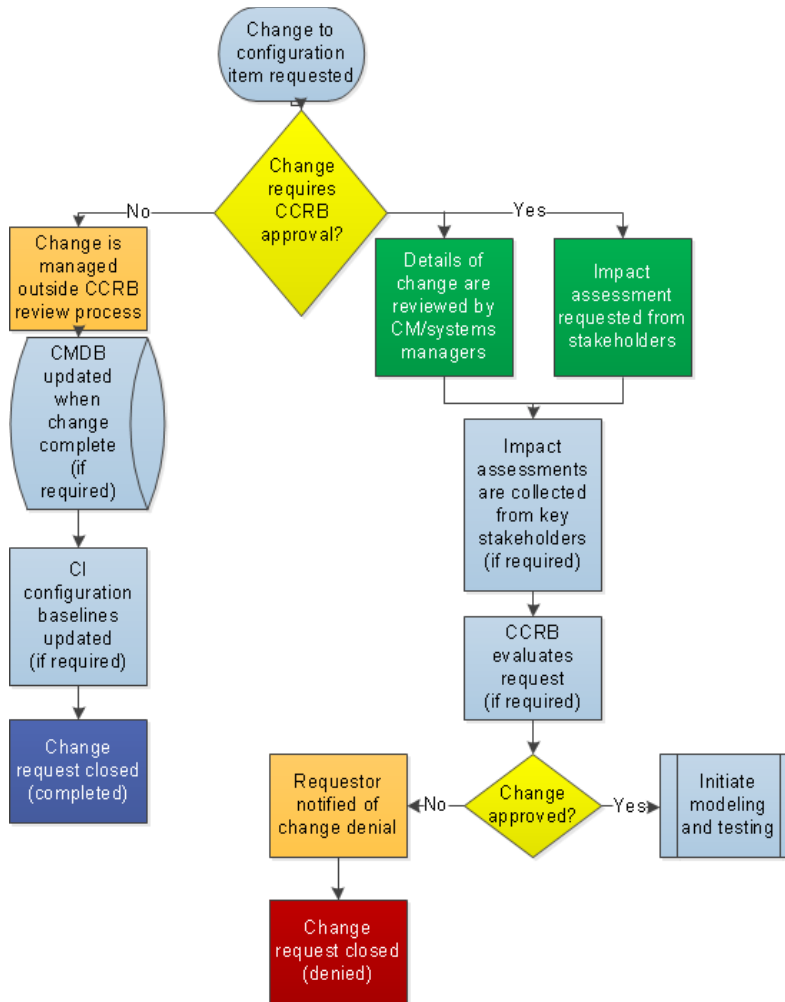
Figure 2: Change Request Evaluation Process

Step 2. Model configuration changes in a test environment.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
Goal 2: The integrity of technology and information assets is managed.	
7. Are modifications to technology assets tested before being committed to production systems? [TM:SG4.SP4]	PR.DS-7: The development and testing environment(s) are separate from the production environment.

The modeling and testing of changes is often an overlooked step in the CM process. Ignoring this step leads to an unusually high occurrence of changes that must be rolled back and a greater number of unsuccessful changes. Organizations with a mature CCM process have an established modeling and test environment for all critical systems, and they document the testing of all changes. An adequate modeling and testing environment should have the following:

- isolated systems whose configurations are identical to the current approved baseline
- data sets that closely mimic those in production (often these are clones of the live data)
  - Follow all regulatory requirements when working even with clones of live data.
  - Document any access of copies of personally identifiable information (PII), financial information, and protected health information.

Distribution Statement A: Approved for Public Release; Distribution is Unlimited

- o Use synthetic data as long as it closely mirrors the structure of actual data.
- inter-system connectivity mirroring that of the production environment (networking, ACLs, access methods)
- access given to system owners and key stakeholders who use the system, but restricted access to all others
- incorporated tools and procedures that test the confidentiality, integrity, and availability of the test data before and after a change is implemented

Adequate testing of large configuration changes may take significant effort. The testing process should not be hastened or modified to save time, except when emergency changes arise. These are addressed later in this section. Figure 3 depicts the modeling and change process.
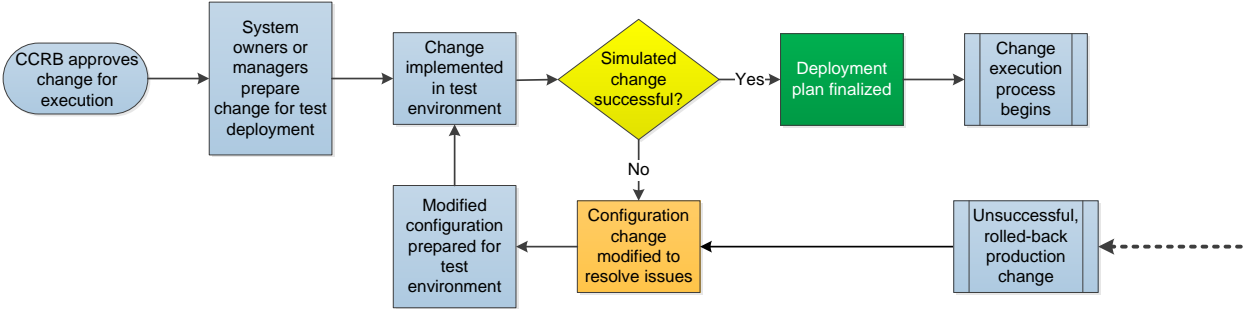
Figure 3: Configuration Change Modeling and Testing Process

When modeling and testing changes, the organization should use the same rigor and discipline as if it were making the changes on a production system. Each step of the change should be documented, along with steps required to roll back the change. These steps will eventually become the procedure for the production deployment. Also, the same automation and monitoring tools should be used, and the same metrics that assess the success of the change should be employed in modeling and testing as in production. These steps and metrics will be aggregated into the configuration deployment plan that will govern the execution of the change onto production systems.

Step 3. Deploy changes in the production environment.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
Goal 1: The lifecycle of assets is managed.	
5. Are stakeholders notified when they are affected by changes to assets? [SC:SG3.SP4]	PR.IP-3: Configuration change control processes are in place.

Configuration changes that are approved by the CCRB and are big enough to require management will then be executed by system administrators using steps A through C below. Figure 4 gives an overview of the change execution process.
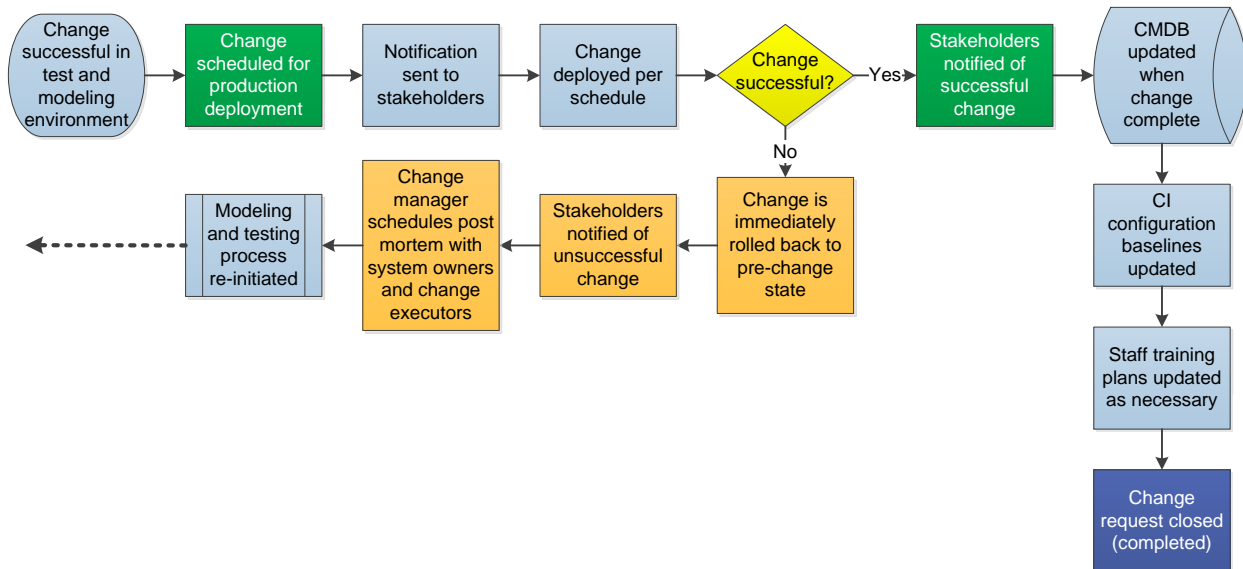
Figure 4: Configuration Change Modeling and Testing Process

A. Schedule configuration changes for deployment into production.
1. Send a general announcement to all staff who have dependencies on the affected system, application, or documentation.
2. Allow adequate time for information to be disseminated to stakeholders.
3. Verify that downtime procedures are in place for mission-critical services.
4. Preferentially schedule configuration changes during non-peak times.
   – Avoid end of month, quarter, or year for financial systems.
   – Avoid peak production times for industrial systems.
   – Avoid times of high patient volume for health-care systems.
   – Avoid critical organizational deadlines or external regulatory audits.

B. Notify key stakeholders immediately prior to the change execution.
1. Prepare on-call or onsite list.
2. Maintain multiple contact avenues for key stakeholders (cell phone, home phone, email, etc.).

C. Deploy changes, following the configuration deployment plan.

Step 4. Determine the success or failure of changes.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
Goal 1: The lifecycle of assets is managed.	
5. Are stakeholders notified when they are affected by changes to assets? [SC:SG3.SP4]	PR.IP-3: Configuration change control processes are in place.

The success or failure of any change depends on several factors. Many of the metrics for these factors are defined when the configuration deployment is developed. The metrics collected as part of the change process can be used to evaluate the overall CCMP as part of the continual improvement process. Examples of change success metrics include the following:
- Did the configuration change have the intended impact on the CI?
- Was the change completed within the window allotted to make the change?

Distribution Statement A: Approved for Public Release; Distribution is Unlimited

- Did the change have to be rolled back due to unidentified issues?
- Did the change have significant, adverse impacts on systems or users not identified prior to the change?
- Did the change have positive or adverse impacts on the confidentiality, integrity, or availability of the data?
- Did the change improve performance of the CI or user experience with the CI?
- Did the communications plan adequately notify stakeholders of the impending change and the progress of the change?
    o This will be largely dependent on the volume of reported issues related to the change.
    o This can also be assessed by using a post-change survey of key stakeholders.

Many other metrics can be used to assess the success of a change. Each organization will need to use metrics that best suit its needs.

Step 5. Roll back unsuccessful changes.

Often configuration changes do not occur as planned. The likelihood of unsuccessful changes can be greatly reduced by deploying all changes in a modeling and test environment (see Step 2 above) prior to any production changes. Even with a robust modeling and testing procedure, some changes will still be unsuccessful in production environments. The organization should take the following steps when a change is unsuccessful:

A. IMMEDIATELY roll back the change to a state prior to the beginning of change execution.
    o Gather any information about the change failure.
    o Restore all configurations for CIs.
    o Restore backups of any changed data to a point immediately prior to the change execution.
    o Execute the testing plan for the system to validate that it is functioning as expected.

B. Notify key stakeholders of the change failure and outline the steps taken to restore expected functionality.
    o Have representatives for stakeholder groups verify the functionality of the systems affected.
    o Notify executive leadership if the impact affects the entire organization.

C. Schedule a post mortem meeting with the change manager, those who executed the change, and any key stakeholders who require situational awareness.

D. The change manager should instruct the change execution team to begin researching alternative ways to execute the change that will be successful.
    o These alternatives should all be tested in the modeling and testing environment.
    o Also consider the impact of not performing the change.

Step 6. Close out completed changes.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
Goal 1: The lifecycle of assets is managed.	
4. Are change requests tracked to closure? [TM:SG4.SP3]	PR.IP-3: Configuration change control processes are in place.

All successful, completed changes should be formally closed out during a meeting of the CCRB. The CCRB should consider the following factors when officially closing out a change:
- Did the change meet its desired objectives and the objectives of the organization?

- Were there any unanticipated impacts of the change?
- Will this change necessitate additional changes?
- Was the change performed within its original budget and resource allocation?
- Are key stakeholders satisfied with the result of the change?
- What can be improved as a result of lessons learned?
  - scheduling
  - process
  - training
  - resource allocation
  - equipment and automation
- Also discuss changes to the configuration baselines of any CIs that were affected by the change.

Addressing Emergency Changes to Configurations

Emergency situations sometimes hasten the configuration change control process. Some examples include
- major incidents (see the Incident Management Resource Guide, Volume 5 of this series)
  - natural disasters (floods, earthquakes, storms)
  - loss of critical supply chain or utility support (material supply vendor outages, electricity, water)
  - technological incidents (denial of service attacks, virus outbreaks, security events, network cable cuts)
  - loss of critical facilities (data center outages, building evacuations for extended periods)
  - external vendor incidents (cloud provider outages, network and telecom provider outages)
- critical security patches released by vendors
- zero-day vulnerabilities that require immediate remediation until a patch can be developed

To effectively mitigate the impact of these events, the organization needs to accelerate its change management process to implement solutions rapidly. This does not mean that all rigor surrounding the change management process should be abandoned. In emergency situations, organizations should consider the following suggestions to quickly implement changes:
- Organize an emergency CCRB that can meet on extremely short notice to approve changes that need immediate implementation.
- Include senior leadership, management of critical lines of business, and management of key IT areas in CCRB membership.
- Plan for multiple methods of meeting (in person, conference bridge, web-meeting) in case the emergency occurs outside normal business hours.
- Create an emergency change implementation plan that includes a list of individuals on the emergency CCRB and a list of procedures that are modified from the standard CCMP.

Certain phases of the implementation process can be compressed to save time, but testing and modeling must still be performed prior to any release of configuration changes into the production environment. Some methods for reducing time to deployment include the following:
- Reduce the number of use cases addressed in modeling and testing.
  - Address several primary use cases, and plan to remediate issues with niche use cases.
  - Perform smaller scale testing in the modeling environment. For example:
    - Deploy patches to 10 test machines instead of 50 or 500.
    - Maintain a list of pilot "superusers" who can more easily acclimate to emergency changes and can communicate temporary remediation tactics to their peers.

- Discuss minimum recovery point objectives (RPOs) with stakeholders for emergency situations. This may reduce the time required to perform backups of systems that may have been recently backed up.
- Utilize emergency downtime procedures to allow systems to be taken completely offline in emergencies. This will allow for outages and reboots in times of heavy utilization to expedite configuration change completion.

> *Example: In a hospital environment, make sure that all medical units have paper downtime procedures that allow patient care to continue during complete outages of IT resources. These procedures should detail any information that needs to be printed prior to the outage and procedures for entering all data back into IT systems once connectivity is restored. Many hospitals also maintain older tube systems that could be used to transmit lab, pharmaceutical, and radiological orders to the appropriate units.*

- Leverage senior management to communicate the urgency of any emergency change and to help achieve rapid consensus for decisions affecting the change implementation timeline.
- Perform periodic emergency drills in the test and modeling environment to mentally prepare IT staff to deal with the additional stress of emergency change. Review the results of these drills and document any improvements to be made from the lessons learned.

Step 7. Change configuration baselines.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
Goal 3: Asset configuration baselines are established.	
2. Is approval obtained for proposed changes to configuration baselines? [TM:SG4.SP3]	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained.
	PR.IP-3: Configuration change control processes are in place.

Once changes are completed successfully and the configuration changes are entered into the CMDB, the organization must update the CI's baseline configuration. This new baseline will be the basis for deployment of any additional instances of that CI, and it will serve as the starting point for any restoration of that CI's configuration.

Note that, in step 1, provisions were made for change requests which did not require CCRB review. The process for managing those change requests should also define whether or not those changes will result in a new baseline configuration.

The change manager and the implementation team should review the new configuration baseline and then formally present it to the CCRB for approval at its next regular meeting. The CCRB should receive documentation on the following:
- differences between the new and currently approved baseline
- benefits of the new baseline
- follow-up changes that should or need to be performed as a result of the new baseline
- possible risks due to the implementation of the new baseline

Once the CCRB reviews and approves the new baseline, the configuration manager should enter the new baseline into the CMDB, along with the implementation date and any relevant details.

Output of Section V

	Output	Guidance
✓	Change request form	See Appendix A for an example. Tailor the form to the organization's needs and include • business justification for change • impacted critical services • key stakeholders • budget or resources required for change • urgency for change or impacts of not performing the change
✓	Impact assessment from key stakeholders	The realization of any anticipated impacts of the change should be documented with the change request: • Did any of these occur? • Were the response or remediation measures sufficient to minimize the effects on stakeholders?
✓	Configuration deployment plan	• Created during modeling and testing process • Includes timing, tools to be used, and rollback procedures • Same tools and metrics are used in testing and production changes
✓	Updates to the CMDB	Successful changes and procedures to enact those changes are documented in the CMDB for future reference.
✓	Emergency CCRB	Contact information for a group of individuals high in the organizational structure who can approve emergency changes for implementation. • Include senior management representation. • Include key line-of-business executives. • Include technical leads from key IT areas (networking, systems, applications, infrastructure). • Technical evaluation is often performed by technical teams in concert with key stakeholders.
✓	Emergency CCMP	A plan that outlines the responsible parties and procedures for enacting emergency configuration changes. • Include differences between the emergency CCMP and the standard CCMP. • Include detail of any known impacts to critical services when emergency change is implemented. • Include emergency downtime procedures if they have been developed. • Tailor emergency CMP to your organization's service-level agreements and the criticality of key services.
✓	Updates to the CI baselines	Successful changes require updates to the current CI baselines. • CCRB must approve all changes to baselines. • Technical teams often perform technical evaluation in concert with baseline updates.

Distribution Statement A: Approved for Public Release; Distribution is Unlimited

VI. Monitor Configuration Changes

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
Goal 2: The integrity of technology and information assets is managed.	
2. Are techniques in use to detect changes to technology assets? [TM:SG4.SP2]	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.

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 monitoring configuration changes.

	Input	Guidance
✓	Audit reports	Reports from recent system audits will outline the current configuration state of the systems.
✓	Approved baseline configuration reports	Used to determine the latest approved baseline for a CI.
✓	Configuration change requests since last audit	Used to verify that all requests have been processed and implemented.
✓	Outstanding configuration change requests	Reports from recent system audits will outline the current configuration state of the systems. Use these audit results to verify that outstanding change requests are still accurately recorded.

Monitoring validates that the system managed by a CCMP is adhering to the approved policies and procedures of the organization. Identifying misconfigurations, unauthorized changes, vulnerabilities, and undocumented systems can reduce the exposure of an organization to unnecessary risks. The use of automated tools will help eliminate mistakes in collecting and organizing data and lead to a more efficient monitoring system.

Step 1. Identify systems or components not specified in documentation.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
Goal 3: Asset configuration baselines are established.	
1. Do technology assets have configuration baselines? [TM:SG5.SP2]	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained.

Scanning of organizational assets will help the organization discover systems and components that are not part of the original recorded inventory. For example, a piece of equipment installed to test a configuration that is never disconnected could provide an unauthorized user access to the infrastructure. Regular scans will alert the

organization to components that may have accidentally or intentionally connected to the organization. When the scans identify unauthorized systems, define

- actions to be taken
- reporting requirements

Step 2. Identify disparities between authorized, approved baselines and actual, implemented baselines.

Scanning will identify the differences between the actual, installed baselines and the documented baselines, which will allow the organization to take action to remediate the issue. For example, an unapproved workstation application that implements several system changes can increase the risk of system compromise. Not all patches or updates can be tested, making the scans valuable for documenting unexpected changes to the baselines. When scanning identifies unauthorized baselines, define

- actions to be taken
- reporting requirements

Step 3. Monitor system logs for unauthorized changes.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
Goal 2: The integrity of technology and information assets is managed.	
5. Is the integrity of information assets monitored? [KIM:SG5.SP3]	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.

Collecting and auditing the system logs for unauthorized access or changes will identify systems that need monitoring or auditing to determine any changes from their approved baseline. Centralized logging that can collect the data and display it in a manner that enables sorting can help identify single changes that have affected one or multiple systems. For example, if a newly installed server application pushed a change out to a number of workstations, a log audit would identify the offending application as well as all the affected workstations. When log audits reveal unauthorized changes, define

- actions to be taken
- reporting requirements

Step 4. Collect existing audits and configuration control records.

The organization should map the existing audits of the systems, including both completed and outstanding configuration change requests, against the current baseline reported by the system scans. Identifying changes that have been approved and implemented but not documented in the system will prevent inconsistencies that lead to improper changes or changes that can adversely affect performance due to configurations that are not compliant with the current baseline. For example, if an application has been updated to the newest version but the change is not documented, a patch that is pushed to a baseline that is directly affected by the current version could lead to unwanted system behavior, including system failure.

Step 5. Define remediation action.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
Goal 2: The integrity of technology and information assets is managed.	
3. Are modifications to technology assets reviewed? [TM:SG4.SP3; TM:SG4:SP2]	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained.
	PR.IP-3: Configuration change control processes are in place.
6. Are unauthorized or unexplained modifications to technology assets addressed [TM:SG4.SP2; TM:SG4:SP3]	PR.IP-3: Configuration change control processes are in place.

Remediation of unidentified or unauthorized systems and configurations can be automated or manual. Automated remediation can remove the offending system from the environment without user intervention, but it can cause system disruptions by taking critical systems offline. Automated remediation can send alerts to system owners or even disconnect the system from the network. Regardless of the action taken, remediation should identify who made the change, determine if the change matches what was approved, document whether the change was accidental or intentional, and identify errors in the implementation.

Step 6. Execute monitoring plan.

Execute the monitoring plan as described in the plan documentation. Once all the results have been collected and analyzed, the plan should be reviewed for identified inconsistencies and shortfalls. The corrective actions should then be documented and the monitoring plan updated to ensure the organizational requirements are being met.
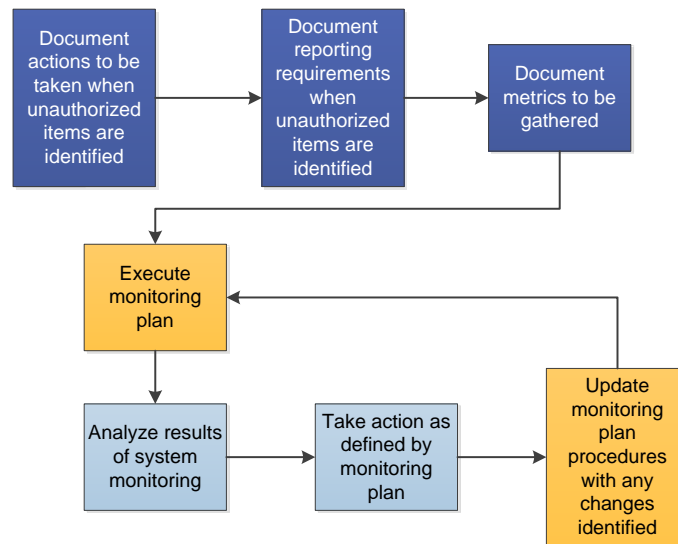

Figure 5: Configuration Change Monitoring Process

Output of Section VI

	Output	Guidance
✓	Implement monitoring program	Implement monitoring program to scan network for unauthorized changes to systems, and define metrics to be gathered.
✓	Identify unauthorized systems	Continuous scans of organizational systems for unauthorized systems not contained in the original inventory. • Define actions to be taken when unauthorized systems are identified. • Define reporting requirements.
✓	Identify disparities between authorized and implemented baselines	Scan systems for baselines that are unauthorized or misconfigured.
✓	Monitor system logs	Monitor system logs for unauthorized access and changes.
✓	Collect existing change documentation	Collect existing documentation that reflects changes to baselines and systems that have been approved or implemented.
✓	Define remedial action	Define actions in response to inconsistencies discovered in systems.
✓	Update plan	Update plan with any procedural changes identified as a result of the system scan.

VII. Conclusion

An organization's assets have many components that are connected in a variety of configurations to provide services that meet a variety of business needs. Managing the risks inherent in the introduction of new systems, or in the upgrading and improvement of existing systems, is critical to the resilience of the organization. Applying patches to existing systems can introduce security vulnerabilities that allow access by unauthorized users and can lead to loss of confidentiality, integrity, or availability of data. Introducing new assets that conflict with current assets can reduce users' productivity by requiring them to enter data into two systems. Establishing and supporting a CCM program enables your organization to evaluate and control the impact of changes that may adversely affect employees, assets, customers, or the security posture of the organization. Many government and private organizations also require CCM, as defined in guidance by FISMA, NIST, FIPS, and HIPAA.

The following documents provide broad program guidance:
- *NIST Special Publication SP 800-128* (http://csrc.nist.gov/publications/nistpubs/800-128/sp800-128.pdf)
- The *CERT Resilience Management Model (CERT-RMM)* [Caralli 2010] is the basis for the CRR and contains more in-depth guidance for establishing practices.

For more information about the Cyber Resilience Review, please email the Cyber Security Evaluation Program at CSE@hq.dhs.gov or visit http://www.us-cert.gov/ccubedvp/self-service-crr.

Appendix A. Example Change Request Template

<Organization Name> Change Request

Title of Change Request:	Change Control ID:
Change Requestor:	Date:

Detailed Description of Change:
Proposed Date / Time of Change:
Stakeholder Groups Impacted:

Business Justification for Change:
Expected Impact of Change:
Expected Impact to Resilience Requirements of Asset:

Rollback Procedures:

Change Urgency: *Low / Medium / High / EMERGENCY*
Justification for emergency change:

Preliminary Assessment by CCRB:

CCRB Decision:

Approved | Rejected | Additional Information Required | Deferred

CCRB Comments:

CCRB Chair Signature:	**Date:**

Appendix B. Example Change Impact Analysis Template

<Organization Name> Change Impact Analysis

Title of Change Request:	**Change Control ID:**
Change Requestor:	**Date:**
Stakeholder Group:	
Analyst:	

Technical Implications:

Stakeholder Groups Impacted:

Business Impact:

Schedule Impact:

Financial Impact:

People Impact:

Resilience Impact:

Organizational Risks of This Change:

Rollback Implications:

Alternatives to Change:

Approved By:	Date:

Appendix C. Configuration and Change Management Resources

Gartner (requires subscription)
http://www.gartner.com/technology/home.jsp
- o Critical Capabilities for Configuration Management Database
  https://www.gartner.com/doc/2770917/critical-capabilities-configuration-management-database

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

ITIL (Requires a Fee)

http://www.itil-officialsite.com/

National Institute of Standards and Technology (NIST)
http://www.nist.gov/index.html
- o NIST Computer Security Division, Computer Security Resource Center
  http://csrc.nist.gov/
  - – Special Publication 800-128, *Guide for Security-Focused Configuration Management of Information Systems*
    http://csrc.nist.gov/publications/nistpubs/800-128/sp800-128.pdf
  - – NIST Special Publication 800-40r3, *Guide to Enterprise Patch Management Technologies*
    http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf

Software Engineering Institute, CERT Division
http://www.sei.cmu.edu/
- o CERT Resilience Management Model
  http://www.cert.org/resilience/rmm.html
- o OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)
  http://www.cert.org/octave/
- o Concepts in Configuration Management Systems
  ftp://ftp.sei.cmu.edu/pub/case-env/config_mgt/papers/cm_concepts.pdf

United States Computer Emergency Readiness Team (US-CERT)
http://www.us-cert.gov
- o Situational awareness information
  https://www.us-cert.gov/

Distribution Statement A: Approved for Public Release; Distribution is Unlimited

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

Table 4 cross-references the CRR Configuration and Change Management 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 4: Cross-Reference of CRR Goals/Practices and NIST CSF Category/Subcategory Against the Configuration and Change Management Resource Guide

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory	Configuration and Change Management Resource Guide Reference
Goal 1: The lifecycle of assets is managed.		—
1. Is a change management process used to manage modifications to assets? [ADM:SG3.SP2]	PR.IP-3: Configuration change control processes are in place.	Section III
2. Are resilience requirements evaluated as a result of changes to assets? [RRM:SG1.SP3]	PR.IP-3: Configuration change control processes are in place.	Section III, Step 7
3. Is capacity management and planning performed for assets? [TM:SG5.SP3]	PR.DS-4: Adequate capacity to ensure availability is maintained.	Section III, Step 3 Section III, Step 11
4. Are change requests tracked to closure? [TM:SG4.SP3]	PR.IP-3: Configuration change control processes are in place.	Section V, Step 6
5. Are stakeholders notified when they are affected by changes to assets? [SC:SG3.SP4]	PR.IP-3: Configuration change control processes are in place.	Section V, Step 3 Section V, Step 4
Goal 2: The integrity of technology and information assets is managed.		—
1. Is configuration management performed for technology assets? [TM:SG4.SP2]	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained.	Section II
2. Are techniques in use to detect changes to technology assets? [TM:SG4.SP2]	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	Section VI
3. Are modifications to technology assets reviewed? [TM:SG4.SP3; TM:SG4:SP2]	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained.	Section VI, Step 5
	PR.IP-3: Configuration change control processes are in place.	
4. Are integrity requirements used to determine which staff members are authorized to modify information assets? [KIM:SG5:SP1]	PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties.	Section III, Step 3
	PR.IP-3: Configuration change control processes are in place.	
	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening).	
5. Is the integrity of information assets monitored? [KIM:SG5.SP3]	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	Section VI, Step 3
6. Are unauthorized or unexplained modifications to technology assets addressed [TM:SG4.SP2; TM:SG4:SP3]	PR.IP-3: Configuration change control processes are in place.	Section VI, Step 5
7. Are modifications to technology assets tested before being committed to production systems? [TM:SG4.SP4]	PR.DS-7: The development and testing environment(s) are separate from the production environment.	Section V, Step 2

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory	Configuration and Change Management Resource Guide Reference
8. Has a process for managing access to technology assets been implemented? [TM:SG4.SP1]	PR.AC: Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	Section III, Step 3
Goal 3: Asset configuration baselines are established.		—
1. Do technology assets have configuration baselines? [TM:SG5.SP2]	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained.	Section VI, Step 1
2. Is approval obtained for proposed changes to configuration baselines? [TM:SG4.SP3]	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained.	Section V, Step 7
	PR.IP-3: Configuration change control processes are in place.	

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. Hunneback, Lou. "Glossary of Terms." *ITIL Service Design (2011 Edition).* The Stationery Office, 2011.