

CRR Supplemental Resource Guide



Volume 2

Controls Management

Version 1.1

Copyright 2016 Carnegie Mellon University

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.

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

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

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

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

DM-0003276

Table of Contents

I. Introduction	1
Series Welcome.....	1
Audience.....	3
II. Controls Management	4
Overview.....	4
Plan for Controls Management	5
Define Controls	5
Analyze and Deploy Controls.....	5
Assess Controls.....	6
Summary of Steps	6
III. Plan for Controls Management	8
Before You Begin.....	8
Step 1. Obtain support for controls management planning	9
Step 2. Establish a controls development strategy.	9
Step 3. Establish a controls identification process.....	14
Step 4. Establish a controls analysis process.....	16
Step 5. Establish a controls assessment process.....	17
Output of Section III	17
IV. Define Controls	18
Before You Begin.....	18
Step 1. Assign responsibility and define enterprise-level controls.	18
Step 2. Assign responsibility and define service- and asset-level controls.	19
Step 3. Document the controls in a security requirements traceability matrix.	21
Output of Section IV.....	21
V. Analyze and Deploy Controls	22
Before You Begin.....	22
Step 1. Analyze existing controls against objectives.....	22
Step 2. Identify gaps.....	23
Step 3. Create and update controls.	24
Step 4. Establish linkages to the risk management process.....	25
Step 5. Update security requirements traceability matrix.....	26
Step 6. Deploy controls.....	26
Outputs of Section V	27
VI. Assess Controls	28
Before You Begin.....	28
Step 1. Staff the assessment process and identify stakeholders.....	28
Step 2. Establish a schedule.....	29
Step 3. Define the scope.....	30

Step 4. Perform the assessment.....30
Step 5. Improve the process.....31
Step 6. Update control objectives and controls.....33
Output of Section VI.....33

VII. Conclusion 34

Appendix A. Security Requirements Traceability Matrix Template 35

Appendix B. Controls Management Resources 36

Appendix C. CRR/CERT-RMM Practice/NIST CSF Subcategory Reference..... 37



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

↔ *This guide*

3. Configuration and Change Management

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, this Controls Management guide outlines tools and activities that identify control objective gaps and residual risks, which can in turn be used in the Risk Management guide.

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 controls management process. To outline this process, this document will use an approach common to many controls management standards and guidelines. The process areas described include

- creating the controls management plan
- defining the controls
- analyzing and deploying the controls
- assessing the controls

More specifically this guide

- educates and informs readers about the controls management process
- promotes a common understanding of the need for a controls management process
- identifies and describes key practices for controls 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.

³ CERT® is a registered mark owned by Carnegie Mellon University.

- II. Controls Management—Presents an overview of the controls management process and establishes some basic terminology.
- III. Plan for Controls Management—Highlights the elements necessary for an effective controls management plan.
- IV. Define Controls—Presents a process for defining controls based on identified objectives.
- V. Analyze and Deploy Controls—Provides a step-by-step approach for controls analysis and deployment.
- VI. Assess Controls—Outlines a process for scheduling, scoping, and performing assessments of controls.
- VII. Conclusion—Provides contacts and references for further information.

Appendices

- A. Security Requirements Traceability Matrix (SRTM) Template
- B. Controls Management Resources
- C. CRR/CERT-RMM Practice/NIST CSF Subcategory Reference

Audience

The principal audience for this guide includes individuals responsible for designing, managing, or deploying cybersecurity resilience controls, including executives who establish policies and priorities for controls management, managers and planners who are responsible for converting executive decisions into plans, and operations staff who implement the plans and participate in the implementation of cybersecurity and resilience controls.

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

II. Controls Management

Overview

The Controls Management domain focuses on the processes by which an organization plans, defines, analyzes, and assesses the controls that are implemented internally. The process depicted in Figure 1 helps the organization ensure the controls management objectives are satisfied.

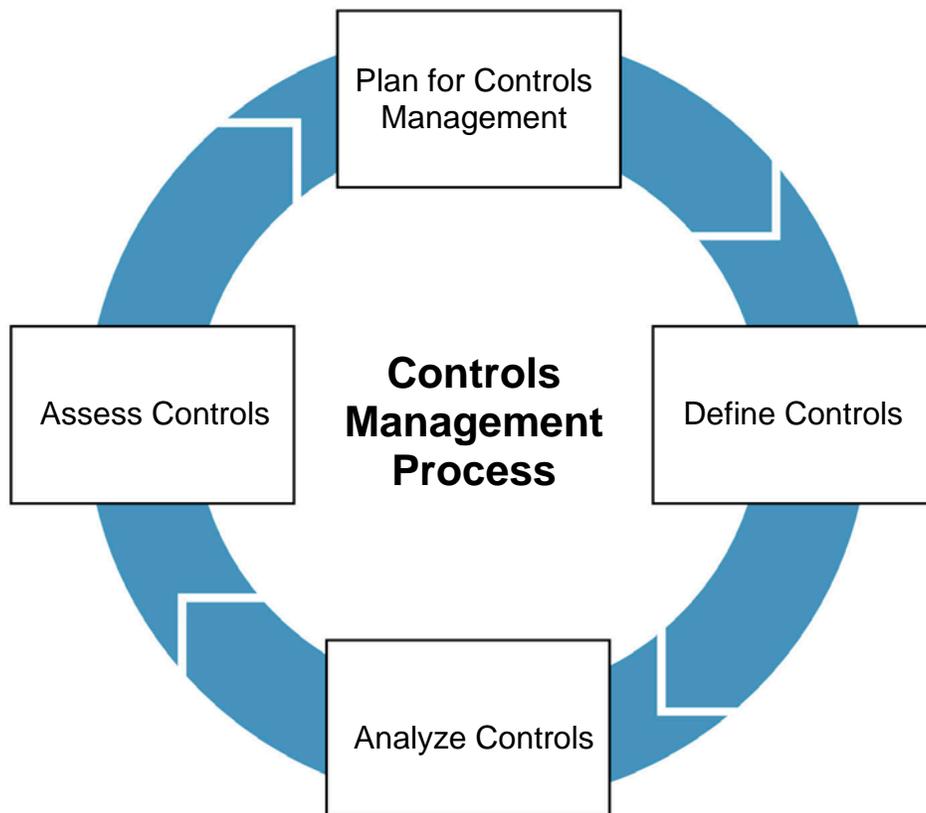


Figure 1: The Controls Management Process

This guide focuses on the resilience controls that allow an organization to operate during a time of stress, rather than financial controls concerning an organization's budgets or return on investments. These resilience controls are implemented in the organization at all levels and require various levels of management and staff to plan, define, analyze, and assess. The high-level outline below highlights the main areas of this domain and points the reader to the corresponding details in this guide.

Plan for Controls Management

Controls management is an intra-organizational governance process that ensures effective achievement of organizational objectives. Control objectives are developed to align with organizational priorities. Operational controls are then developed to meet the control objectives, which help ensure the resilience of assets and the services they support. Enterprise controls, which apply universally across the entire organization, are also developed. Additionally, all controls can be categorized as administrative, technical, or physical.

Controls management typically takes place at various levels of an organization. Enterprise controls are developed to address organization-wide directives but are typically implemented by the operating units. Operational controls are typically developed and implemented at the operating units. Regardless of the level where the controls are developed and implemented, management support at all levels is essential to an effective controls management program. Management must support the process for it to filter down to the rest of the organization. With management's support, processes are defined to identify, implement, and assess controls on an ongoing basis to ensure the resilience of services and the assets that support them.

Important activities while planning for controls management include the following:

- Obtain support for controls management planning.
- Establish a controls development strategy.
- Establish a controls identification process.
- Establish a controls analysis process.
- Establish a controls assessment process.

Define Controls

Controls are derived to meet the control objectives. Responsibility for defining enterprise-, service-, and asset-level controls needs to be assigned to the appropriate organizational units and people. Service- and asset-level controls are defined within each operating unit based on their priority to operational resilience. Section IV identifies the process for defining controls of various types and mapping them to their objectives.

Important activities for defining controls include the following:

- Assign responsibility and define enterprise-level controls.
- Assign responsibility and define service- and asset-level controls.
- Document the controls in a SRTM.

A control objective is a performance target for a control. Control objectives reflect management's directives and are used to select, analyze, and manage an appropriate mix of controls.⁴

Analyze and Deploy Controls

The analysis of existing controls within the organization should focus on ensuring the controls meet the control objectives. Establishing and properly analyzing control objectives at a service level will enable the organization to ensure that one or more service-level and asset-level controls are implemented for the service.

Service refers to a set of activities that the organization carries out in the performance of a duty or in the production of a product. Asset refers to something of value to the organization, typically people, information, technology, and facilities that the service relies on.⁵

Organizations must regularly analyze their control environments to ensure that control objectives are achieved. The methods for analyzing controls will vary greatly, and organizations should consider their objectives, the technology utilized, and budget constraints when selecting a method. Section V offers a list of analysis techniques and tools for the organization to consider.

Important activities for analyzing the controls management process include the following:

- Analyze existing controls against objectives.
- Identify gaps.
- Create and update controls.
- Establish linkages to the risk management process.
- Update SRTM.
- Deploy controls.

Assess Controls

In the assessment phase of the controls management process, the organization should focus on ensuring that the deployed controls in the internal control system support the control objectives and, by extension, meet resilience requirements. Assessing the controls will allow the organization to determine if the controls in place are functioning effectively.

Section VI gives an overview of effectively planning assessments and the pros and cons of various assessment methods.

Important activities in the controls management assessment process include

- Staff the assessment process and identify stakeholders.
- Establish a schedule.
- Define the scope.
- Perform the assessment.
- Improve the process.
- Update control objectives and controls.

Summary of Steps

The following sections of this guide lay out the discrete steps for developing a plan to implement the controls management process as described above:

Plan for Controls Management

1. Obtain support for controls management planning.
2. Establish a controls development strategy.
3. Establish a controls identification process.
4. Establish a controls analysis process.
5. Establish a controls assessment process.

Define Controls

1. Assign responsibility for and define enterprise-level controls.
2. Assign responsibility for and define service and asset-level controls.
3. Document the controls in a SRTM.

Analyze and Deploy Controls

1. Analyze existing controls against objectives.
2. Identify gaps.
3. Create and update controls.
4. Establish linkages to the risk management process.
5. Update SRTM.
6. Deploy controls.

Assess Controls

1. Staff the assessment process and identify stakeholders.
2. Establish a schedule.
3. Define the scope.
4. Perform the assessment.
5. Improve the process.
6. Update control objectives and controls.

Organizations that already have a controls management program can assess and improve it by using the guidance in this resource guide.



III. Plan for Controls Management

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 controls management program.

	Input	Guidance
✓	Scoping statement	This statement defines what the controls management program and plan need to address. Controls management should cover, at a minimum, all critical organizational services. Organizations that are not sure where to start should focus on the most essential services and the areas that directly affect their mission. This approach may allow an organization to address the areas of greatest risk first and mitigate their impact while control objectives and associated controls are being defined for noncritical areas. If your organization has participated in a CRR, it may be beneficial to begin with the critical service addressed during the CRR. See Appendix C for a cross-reference between the CRR and this guide.
✓	List of stakeholders	The list of stakeholders should be aligned to the scoping statement and include all appropriate internal and external entities. Potential candidates include <ul style="list-style-type: none"> • executive and senior management • heads of business lines, especially critical services owners • information technology • legal • board of directors • technology vendors • regulators and auditors • compliance personnel
✓	Management support	An endorsement by senior management for establishing a controls management program and implementing processes
✓	An understanding and acknowledgement of an acceptable approach to controls management	Acknowledgement from management for the intended approach to controls management, including stakeholder expectations about acceptable risk tolerance for the identified critical assets and services
✓	Externally imposed requirements for controls management	<ul style="list-style-type: none"> • Regulatory requirements defining mandatory controls assessments and other needs • Service-level agreement requirements
✓	List of critical assets and services	To define control objectives, the critical assets and services need to be identified.
✓	Risks	Obtain the list of categorized and prioritized risks.
✓	Linkage between asset types	Multiple asset types such as people, information, technology and facilities typically support critical assets and services. The linkage between these asset types and the critical asset or service should be identified.

✓	Assignment of responsibility for controls management	Job descriptions for roles that have responsibilities for controls management, for example, executive ownership, decisions, communication, testing, and disruption risk management
✓	Budget for controls management	Identification of available funds to perform controls management planning and execution, including <ul style="list-style-type: none"> • staffing resources • tools (applications and associated hardware) • third-party support

Step 1. Obtain support for controls management planning.

Obtaining support from management is essential to ensuring the controls management plan is effectively implemented. A top-down approach is often helpful in ensuring the controls management program meets the resilience objectives of the organization.

The level of management support required depends on the scope of the controls being implemented. Senior-executive-level support is necessary for a controls management plan that addresses the entire organization. Smaller implementations, such as those at the service level, may require only sponsorship from management responsible for that particular service. To illustrate, consider an electric utility company that has four main services: generation, transmission, distribution, and business support. A controls management program could be implemented for these services individually. When the scope is limited to a single service or component of an organization, the involvement and support of the organization’s senior management may be limited, and more involvement might be required from officials within the individual service or component.

Step 2. Establish a controls development strategy.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
Goal 1: Control objectives are established.	
1. Have control objectives been established for assets required for delivery of the critical service? [CTRL:SG1.SP1]	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.
	PR.AC: Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.
	PR.DS: Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.
	PR.IP: Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.
	PR.MA: Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.
	PR.PT: Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.
2. Are control objectives prioritized according to their potential to affect the critical service? [CTRL:SG1.SP1]	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.
	PR.AC: Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.

	PR.DS: Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
	PR.IP: Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.
	PR.MA: Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.
	PR.PT: Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

A. Establish a controls objective definition process. Control objectives are broad-based targets for the effective and efficient performance of controls. Organizations use control objectives to select the type, number, and mix of controls to ensure the organization's strategic objectives are being met. Control objectives should be developed to reflect priorities at the enterprise and operating-unit levels as well as for specific critical services. Control objectives will vary depending on the level of the organization at which the objective was defined and the process in question. The following steps illustrate the process for establishing a control objective definition process:

- i. Identify management directives and organizational priorities. Organizational priorities can be articulated in many forms and help identify the strategic objectives. Strategic objectives are derived from strategic planning activities, which usually forecast two to five years out.⁶ The following sources can provide insight into management directives and organizational guidelines:
 - o strategic plan: The document in which an organization defines its plans for achieving its mission, where the organization wants to go, and how it plans on getting there.⁷ Large enterprises may have strategic plans at multiple levels within the organization such as the enterprise and operating-unit levels.
 - o critical success factors (CSFs): A small number of areas an organization must consistently perform well in to meet its goals and mission.⁸ CSFs illustrate what the organization considers its top priorities in achieving its goals.
 - o legal and regulatory obligations: Legal and regulatory obligations will often give insight into requirements placed on the organization from external entities.⁹
 - o internal policies and procedures: Policies and procedures developed by the organization to promote acceptable behaviors and practices.¹⁰

See the Risk Management Resource Guide, Volume 7 of this series. Also see the Risk Management (RISK) process area in the CERT-RMM for more detailed guidance on deriving resilience objectives.

- ii. Define and document control objectives derived from management directives and guidelines. Control objectives will be derived from the management directives and organizational priorities identified above. Control objectives provide a set of high-level requirements to be considered for effective control of each critical asset and/or service. Control objectives should
 - o state management intentions to increase value and reduce risk
 - o consist of organization and operating-unit policy and procedures
 - o provide reasonable assurance that objectives will be achieved and undesired events will be prevented or detected and corrected¹¹

To ensure operational resilience, an organization should consider each of the four asset types—people, information, technology, and facilities—when developing control objectives. Table 1 maps the asset types to example control objectives.

Table 1: Asset Types Mapped to Example Control Objectives

Asset Type	Control Objective Example
People	Ensure all employees are trustworthy and reliable before hiring them.
Information	Ensure the confidentiality of customers' payment information.
Technology	Ensure the databases, which support one or more critical services, remain available.
Facilities	Ensure environmental systems are maintained at an appropriate level to support data center equipment.

Control objectives should be aligned with the strategic objectives, organizational risk tolerance, and resilience requirements of high-value assets. An organization uses risk tolerance thresholds to determine if risk is being adequately managed or is exceeding an acceptable level, requiring management action to reduce the organization's exposure to the risk.

See the Risk Management Resource Guide, Volume 7 of this series. Also see the Risk Management (RISK) process area in the CERT-RMM for more detailed guidance on risk thresholds.

iii. Prioritize control objectives. Control objectives should be prioritized based on their potential to affect operational resilience.¹² This prioritization of control objectives will help the organization determine the allocation of resources, such as the number of controls and time spent monitoring and assessing them, to the controls that address the high-priority services and assets. The following steps illustrate the process for prioritizing control objectives:

- a. Inventory high-value assets:
 - vital staff
 - high-value information
 - high-value technology
 - high-value facilities¹³

See the Asset Management Resource Guide, Volume 1 of this series. Also see the Asset Definition and Management (ADM) process area in the CERT-RMM for more detailed guidance on identifying high-value assets.

- b. Inventory high-value services:
 - inventory of services
 - document of service attributes
 - affinity analysis of organizational services and objective measures
 - defined high-value services¹⁴

See the Service Continuity Resource Guide, Volume 6 of this series. Also see the Service Continuity (SC) process area in the CERT-RMM for more detailed guidance on prioritizing business services via a business impact analysis.

- c. Obtain the list of categorized and prioritized risks.
- d. Prioritize control objectives. Control objectives should be prioritized using the list of high-value assets and services as well as the list of prioritized risks for each category.

See the Risk Management Resource Guide, Volume 7 of this series. Also see the Risk Management (RISK) process area in the CERT-RMM for more detailed guidance on categorizing and prioritizing risk.

It is also important to understand the linkage between asset types and the critical services that they support. For example, an electric utility may identify electric generation as a critical service. When prioritizing control objectives, the utility needs to account for the assets that support this critical service such as the engineers and operators who maintain the supervisory control and data acquisition (SCADA) system, the SCADA system set points stored on the internal servers, the SCADA hardware and software, and the plant housing the control system. Figure 2 illustrates the relationship between a critical service and its underlying assets.

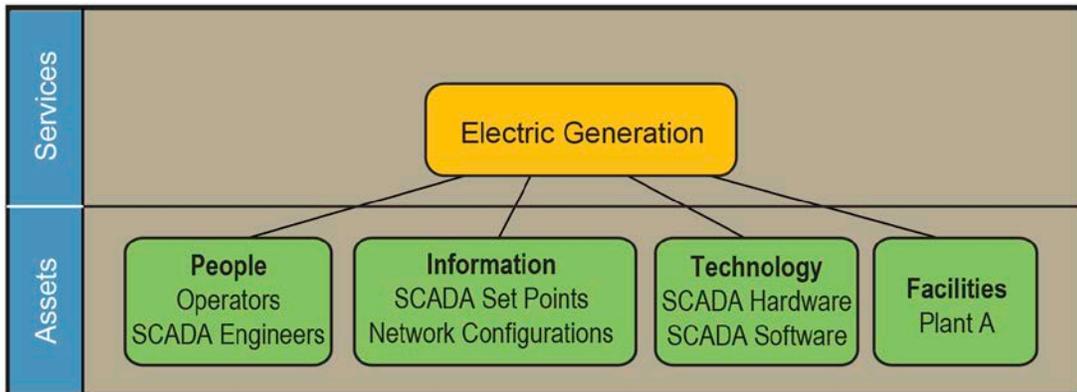


Figure 2: Example Service and Asset Relationships

- B. Establish a controls development strategy.** The resources available to an organization for controls management will influence the strategy selection. The controls development strategy should
- focus on increasing the resilience of critical assets and services
 - align with the organization’s strategic objectives

Before controls are established, it is important to understand the different types of controls and when they should be used. Enterprise-level controls apply universally across the entire organization. Operational controls ensure the resilience of services, including the assets that support those services. All controls can be categorized as administrative, technical, or physical:

- administrative controls—Administrative controls typically set and enforce management’s policies and have to be paired with technical and physical controls to be effective.¹⁵ Enterprise-level controls are often administrative; however, administrative controls can exist at the level of operating units or individual services. Examples of administrative controls are
 - governance
 - setting policy
 - monitoring
 - auditing
 - enforcing
 - separation of duties
 - developing and implementing service continuity plans¹⁶
- technical controls—These controls are operational in nature and primarily executed through information technology components such as hardware, software, and firmware.¹⁷ Examples of technical controls are
 - network access control

- complex passwords
- error checking
- host-based intrusion detection system

Technical controls can often be more general than those implemented for a specific technology or platform. These types of technical controls are referred to as IT General Controls.¹⁸ Within a large enterprise, the IT department often provides technical controls as common services to the rest of the organization. Often the effective operation of application-specific controls depends on technical controls functioning as intended. Examples of IT General Controls are

- systems development
 - change management
 - security
 - computer operations¹⁹
- physical controls—These are controls for the physical environment and protect people as well as facilities and the services and technology within. Examples of physical controls are
 - guards
 - closed circuit television (CCTV)
 - biometric access
 - temperature and humidity control

An organization can use a single controls development strategy or elements from multiple strategies as long as the selected approach aligns with the strategic objectives of the organization. The organization should decide on the best strategy for identifying controls to address the risks. The strategy could consist of adopting controls from an existing controls catalog, such as NIST SP 800-53 low-level controls, for a particular service. For areas requiring more protection, moderate- and high-level NIST 800-53 controls could be added, or unique controls could be developed.

An alternative strategy might focus more resources on controls within a particular control type. For example, an organization might dedicate more resources to preventive controls, such as strong physical and logical security, and not apply as many resources to detective controls. An organization can apply any mix of strategies as long as the approach aligns with the organization's strategic objectives and can be implemented with its available resources.

The four control types are

- preventive—prevent unwanted actions
- detective—detect unwanted acts; often used in after-the-fact investigations
- corrective—help fix a previously discovered problem and prevent its recurrence
- compensating—provide a level of redundancy to a control group; compensating controls can be of any control type

The layering of controls is an important concept that should be considered when implementing a controls management program. Organizations may find that preventive controls are the most essential because they offer robust protection to critical assets, but organizations should not overlook the need for detective controls. Layering controls, such as having detective controls in place to supplement preventive controls, can also help to control costs. Establishing an effective mix of controls should be considered as a way to keep costs down when developing and evaluating potential controls. Figure 3 shows an example of how a

fictitious organization—in this case an electric utility—might layer controls to protect its SCADA technology and software.

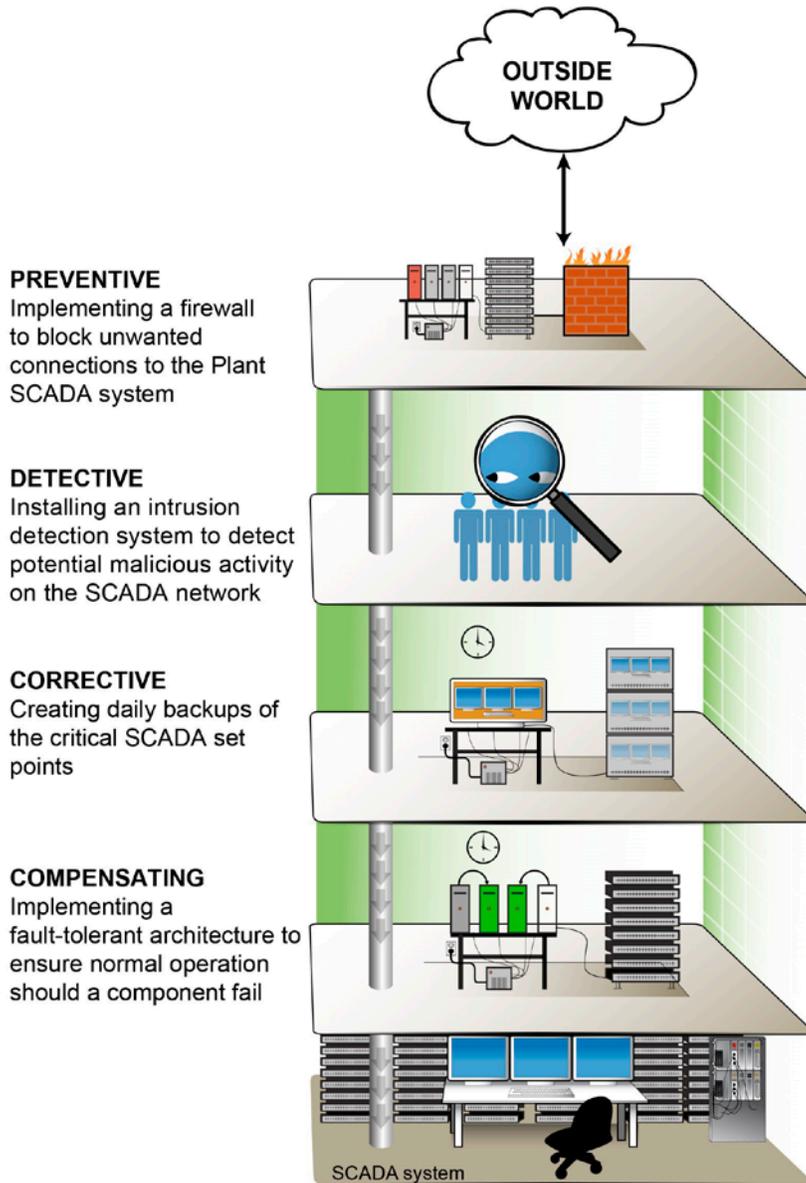


Figure 3: Control Layering Example

Step 3. Establish a controls identification process.

The purpose of a controls identification process is to identify specific controls that can implement the controls development strategy mentioned previously. When identifying controls, it is important to have an understanding of the organization’s asset management processes, which should include an inventory of assets. To effectively identify controls, an organization must establish an inventory that documents the assets and identifies which are critical to the services the organization provides. It must consider asset management when developing controls to ensure that its controls management process allocates sufficient resources to the critical

assets. As discussed above, implementing controls can be a costly process, so an organization should consider its defined resilience requirements and the criticality of assets when instituting a process for establishing controls.

See the Asset Management Resource Guide, Volume 1 of this series. Also see the Asset Definition and Management (ADM) process area in the CERT-RMM for additional information on managing and defining high-value assets and services they support.

The following steps illustrate the process for establishing controls:

- A. Before implementing new controls, review the existing controls to ensure new controls are not redundant.** Enterprise-level controls are often common controls that can be inherited by critical assets and services across the organization.
- B. Review existing controls to determine if they are still effective.** This review is often completed as a by-product of auditing activities. Control assessment activities should provide sufficient evidence to determine the effectiveness of the implemented controls.
- C. Establish new controls to fill the gaps between existing and updated controls.**
- D. Confirm existing and updated controls, and assign responsibility for implementing new controls.** Responsibility for ensuring that enterprise controls are implemented typically rests with the operating-unit managers.

When identifying and establishing potential controls, it is important to remember that a control can often apply across multiple processes, systems, and/or assets in multiple operating units throughout the enterprise. These controls are referred to as *common controls*. Common controls are those which, once implemented, provide a security function that is inheritable by other organizational systems and processes. Enterprise-level controls apply across the enterprise, while common controls can be implemented at various levels. Common controls are often at the enterprise level; however, individual business units can implement common controls, which would then apply to systems and processes within that business unit. Policies and procedures developed and implemented at the enterprise level could be common to an entire organization; but, for example, a policy developed by the finance department that mandates multifactor authentication for all financial applications is not an enterprise control but would be inheritable, and therefore common, by all of those applicable systems in the finance department. Table 2 lists examples of potential common controls.

Table 2: Common Control Examples

Common Control	Control Type	Explanation	Commonality
Security awareness training	Preventive	Security awareness training educates users and can thus prevent attacks	Typically mandated for the entire enterprise, making it a candidate for a common control
Rules of behavior	Preventive	Rules of behavior educate users on what is acceptable use of IT equipment thereby discouraging unacceptable behavior	Typically mandated by the enterprise and/or operating unit, making it a common control
Intrusion Detection System (IDS)	Detective	An IDS monitors the network to detect suspicious traffic	Typically managed by an IT department for an entire enterprise or operating unit, making it common across the applicable organizations
Audit log monitoring	Detective	Audit log monitoring tools analyze audit logs to detect suspicious activity	Typically managed by an IT department for an entire enterprise or operating unit, making it common across the applicable organizations
Drive mirroring	Corrective	SAN solutions required for mirroring allow flaws to be easily corrected	Typically managed by an IT department for an entire enterprise or operating unit, making it common across the applicable organizations
Configuration management tools	Corrective	Enforce standard configurations and correct machines that are not in compliance	Typically managed by an IT department for an entire enterprise or operating unit, making it common across the applicable organizations

To further put common controls into perspective, take a large enterprise with multiple operating units consolidated onto one campus. The physical security and environmental controls will likely be controlled by one operating unit responsible for the controls affecting these services. Because the other operating units share the facility, they can inherit the results of these implemented controls.

Step 4. Establish a controls analysis process.

In a controls analysis process, an organization analyzes the proposed and existing controls to ensure they are meeting the control objectives.²⁰ The level of analysis should vary based upon the resilience requirements for the applicable asset or service. The following steps highlight the controls analysis process. Section V provides detailed steps on controls analysis.

1. Analyze existing controls.
2. Identify gaps.
3. Create and update controls.
4. Identify risks.

See the Risk Management Resource Guide, Volume 7 of this series. Also see the Risk Management (RISK) process area in the CERT-RMM for additional information on managing risks.

Step 5. Establish a controls assessment process.

The controls assessment process involves identifying and evaluating security controls to ensure the effectiveness and efficiency of services and the assets that support them.²¹ The following steps outline the control assessment process. Section VI provides detailed steps on control assessments.

1. Staff the assessment process and identify stakeholders.
2. Establish a schedule.
3. Define the scope.
4. Perform the assessment.
5. Improve the process.
6. Update control objectives and controls.

Output of Section III

	Output	Guidance
✓	Management directives and guidelines	Management directives and guidelines should be clearly identified.
✓	Prioritized controls objectives	Using the management directives and guidelines, list of critical assets and services, and the asset types that support them, a prioritized list of control objectives should be defined.
✓	Control development strategy	Organizations should identify the appropriate mix of control types and adequate layering.
✓	Controls identification process	Controls are identified that meet the control objectives.
✓	Controls analysis	A process is developed for analyzing controls to identify gaps between the control objects and identified controls.
✓	Controls assessment process	A controls assessment process is identified and documented using the steps above.

Once your organization has documented its controls management plan, standards, and guidelines, it should periodically review and update them, at least annually or as required by regulation or other guidelines, to ensure that they are achieving the desired results.



IV. Define Controls

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 defining controls.

	Input	Guidance
✓	Lists of stakeholders	The list of stakeholders should be aligned to the control objectives. Potential candidates include <ul style="list-style-type: none"> • executive and senior management • other affected critical asset and services owners • information technology service owners
✓	Critical assets identified and documented	People, information, technology, and physical assets are identified and documented. See the Asset Management Resource Guide, Volume 1 of this series, for more information on defining and documenting the critical assets.
✓	Control objectives	<ul style="list-style-type: none"> • enterprise-level control objectives • service-level control objectives • asset-level control objectives

Step 1. Assign responsibility and define enterprise-level controls.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
Goal 2: Controls are implemented.	
1. Have controls been implemented to achieve the control objectives established for the critical service? [CTRL:SG2.SP1]	<p>ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.</p> <p>PR.AC: Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.</p> <p>PR.DS: Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.</p> <p>PR.IP: Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.</p> <p>PR.MA: Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.</p> <p>PR.PT: Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.</p>

Enterprise-level controls are high-level controls that are derived from enterprise-level control objectives.²² The overall approach to controls management is established at the enterprise level. This approach is defined and communicated throughout the enterprise through policies and directives issued by senior management.²³ Responsibility for ensuring that enterprise control objectives are implemented typically rests with the operating-unit managers. These controls are typically addressed through policies and procedures applicable to those levels of the organization that focus on implementing the enterprise-level control objectives. Enterprise-level controls typically have the following characteristics:

- based on enterprise-level policies
- apply to all business and operating units
- somewhat general level of detail

For example, an enterprise-level control might require that all major systems and applications undergo an annual audit that includes an assessment of the applicable security controls. This control would be implemented at the operating units, with a policy mandating annual control assessments for all major systems and applications and providing details for how these assessments will take place.

Step 2. Assign responsibility and define service- and asset-level controls.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
Goal 2: Controls are implemented.	
1. Have controls been implemented to achieve the control objectives established for the critical service? [CTRL:SG2.SP1]	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.
	PR.AC: Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.
	PR.DS: Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
	PR.IP: Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.
	PR.MA: Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.
	PR.PT: Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

Service-level controls are defined to meet control objectives that support critical services. Controls management uses these services and their prioritization to allocate an appropriate mix of controls to ensure that high-value services remains resilient. Service-level controls are typically an aggregate of the controls of the service's supporting assets.²⁴ The following is an example of a service-level control objective and its associated controls:

service-level objective: Only authorized individuals with a valid need are given access to the facility.

- service-level controls that support the objective:
 - Managers fill out an online form requesting physical access to the facility for employees with a valid need. Access requests must be approved by a director and implemented by a facilities officer.

- A facilities officer must perform monthly audits on the access logs to ensure that all employees accessing the facility are authorized and have a valid need for the access.
- The monthly audit must be presented to and signed off by the facility director.

The following steps illustrate the process for establishing service-level controls:

- A. Before implementing new controls, an organization should review the existing controls to prevent redundancy.** Existing service-level controls are derived from asset-level controls supporting the critical service.²⁵
- B. Review existing service-level controls to see if they can be updated in a way that will increase their usefulness while keeping down costs.**
- C. Establish new service-level controls to fill the gaps between existing and updated controls.**

Asset-level controls protect and sustain the asset required for a critical service.²⁶ Asset-level controls can apply to all asset types. The service and asset owners are usually responsible for implementing service- and asset-level controls. Table 3 provides examples of asset-level controls.

Table 3: Examples of Asset-Level Controls

Asset Type	Administrative Controls	Technical Controls	Physical Controls
People	<ul style="list-style-type: none"> • Personnel screening • Access agreements 	—	<ul style="list-style-type: none"> • Physical access controls • Emergency lighting
Information	<ul style="list-style-type: none"> • Information security policies • Training to ensure proper information handling 	<ul style="list-style-type: none"> • Role-based access controls 	<ul style="list-style-type: none"> • Clean screen policies
Technology	<ul style="list-style-type: none"> • Policies that govern users' behavior with regard to information technology assets • Logging, monitoring, and auditing 	<ul style="list-style-type: none"> • Hashing to ensure file integrity 	<ul style="list-style-type: none"> • CCTV
Facilities	<ul style="list-style-type: none"> • Facility access procedures • Evacuation procedures 	<ul style="list-style-type: none"> • Card readers providing physical access 	<ul style="list-style-type: none"> • Physical barriers around the facility

Consider a facility with various types and layers of controls in place to protect the facility, technology, information, and people assets. Preventive controls include the security fence around the perimeter, CCTV, a secured data center, and a firewall to protect the technology assets. Detective controls include an intrusion detection system (IDS), which protects the information assets, and corrective controls include an alternate site to serve as a backup should the main facility become unavailable.

Control layering is an important concept in a controls management program. Layering involves using multiple control types to enhance operational resilience. The example facility has a firewall to prevent a network-based attack. The facility's IDS should detect any suspicious events that make it past the firewall. The layering of controls is essential to the operational resilience of critical services and assets.²⁷

Another important concept to understand is defense-in-depth, which has been defined as “the synergistic integration of layered Information Assurance practices, providing resilient IT services while minimizing failures and intrusions.”²⁸ Think of it as deploying multiple layers of controls to protect against the failure of

one. For example, the main building of the example facility is a controlled-access facility with a data center that is a secured room with controlled access. The overall defense-in-depth program—the security fence, CCTV, guards, electronic access systems, and other controls—protects the main building, data center, equipment, and information. Additionally, while the individual computers may be protected by host-based firewalls, they are also protected by a defense-in-depth strategy provided by the enterprise network, which includes logical access controls, network segmentation, multiple firewalls, IDSs, and other controls.

A few of the obvious controls are listed below:

- Preventive
 - security fence protecting the facility assets
 - secured data center inside the building protecting the technology assets
 - firewalls protecting the information assets
 - fire suppression system protecting the people assets
- Detective
 - CCTV protecting the facility assets
 - IDS protecting the information assets
 - fire detection system protecting facility assets
- Corrective
 - an alternate site as a corrective control for the facility assets
 - data mirroring to alternate facility as a corrective controls for the information assets
 - backup equipment for critical devices as a corrective control for the technology assets

Step 3. Document the controls in a security requirements traceability matrix.

Organizations should use a SRTM to map the controls to the control objectives. The SRTM correlates control objectives to controls and ensures that at least one control maps to each objective. The essential data found in the SRTM includes the control objective, authority, test objectives, and the verification methods for these objectives. Appendix A provides a SRTM template that can be used to map control type, control objectives, control activities, control testing procedures, and authority.

Output of Section IV

	Output	Guidance
✓	Responsibility for defining controls	<ul style="list-style-type: none"> • Enterprise controls assigned in management policies and directives • Service- and asset-level controls assigned in policies and procedures at these process areas
✓	Defined controls	Enterprise-, service-, and asset-level controls defined
✓	Security requirements traceability matrix	Matrix depicting control objectives and associated controls that satisfy those objectives



V. Analyze and Deploy Controls

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 analyzing and deploying the controls.

	Input	Guidance
✓	Prioritized list of control objectives	A prioritized list of control objectives the organization has determined will increase its operational resilience
✓	Defined controls	A list of defined controls the organization has chosen that satisfy the control objectives
✓	Security requirements traceability matrix	Matrix depicting control objectives and associated controls that satisfy those objectives

Step 1. Analyze existing controls against objectives.

After defining the controls, the organization should execute its analysis process to ensure the controls satisfy one or more of the control objectives and that they are operating as intended within the internal controls system. Both existing and proposed controls should be analyzed. The analysis should be based on the control objective prioritization outlined in the organization’s control management plan. High-priority control objectives may require more analysis than lower priority objectives. It is important for the organization to determine the level of analysis necessary. Controls analysis can be achieved many different ways. Two methods for consideration are

1. subjective review
 - review of policy and procedures to ensure they are satisfying the intent of the control objective
 - design reviews
 - facility walk through
 - personnel interviews (provides an opportunity to speak directly with asset and service owners)
2. formalized test procedures
 - formal penetration testing at the facility
 - asset-level test procedures (e.g., firewalls, network/host intrusion detection)
 - configuration benchmarks
 - factory acceptance tests
 - site acceptance tests

There are many other places for an organization to find information on analyzing controls. As a starting point, the organizations listed in Table 4 offer tools and documents.

Table 4: Analysis Tools and Documents

Organization	Tools	Use Cases
Center for Internet Security (www.cisecurity.org)	<ul style="list-style-type: none"> security configuration benchmarks benchmark assessment tools security metrics 	Organizations looking to implement baseline configurations and tools to test those baseline configurations should consider the Center for Internet Security tools.
National Institute of Standards and Technology (www.nist.gov)	<ul style="list-style-type: none"> NIST SP 800-53 <i>Recommended Security and Privacy Controls in Federal Information Systems</i> NIST SP 800-53A <i>Guide for Assessing the Security Controls in Federal Information Systems</i> 	Organizations looking for a standard set of controls, developing test criteria, and assessing those controls should consider using NIST SP 800-53 and NIST SP 800-53A.
Information Systems Audit and Control Association (www.isaca.org)	<ul style="list-style-type: none"> COBIT Framework 	Organizations looking for a starting place to develop control objectives and performance measures should consider COBIT.

Controls management analysis relies heavily on the work that created the controls management plan. It is important for the organization to prioritize objectives during the analysis phase.

Step 2. Identify gaps.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
Goal 3: Control designs are analyzed to ensure they satisfy control objectives.	
1. Are control designs analyzed to identify gaps where control objectives are not adequately satisfied? [CTRL:SG3:SP1]	PR.IP-7: Protection processes are continuously improved.

The process of identifying gaps is a critical component of the controls management process. It allows an organization to ensure that the controls currently in place are satisfying the control objectives, and it feeds the improvement process for the organization’s controls management program.

The following are examples of gaps that should be considered and documented:

- A control does not fully meet one or more control objectives.
- An enterprise-level control objective is not satisfied by one or more controls.
- A service control objective is not adequately satisfied by one or more service- or asset-level controls.

Table 5 shows examples of likely gaps when deploying a controls management program.²⁹

Table 5: Example Controls Gaps

Control Objective	Gap Identified
Ensure all employees are trustworthy and reliable prior to hiring them.	Resource limitations or constraints—The methods and rigor with which background checks can be conducted is limited. The organization may be able to do only a high-level check (application references) compared to obtaining a government clearance.
Access to the network and any network-connected system (e.g., file and print services, application servers, database servers) is controlled to prevent access by unauthorized entities.	Lack of adequate infrastructure or supporting processes and technology—The organization may have legacy hardware/software installed that does not support the latest technology.
The network access list consists only of current users, and users are deleted from the list within 60 days when they no longer need access.	Insufficient period of review for controls in place—The organization has determined that users are to be deleted from the list within 30 days of no longer requiring access.

Control gaps should be identified, documented, and addressed before the controls are deployed. Gap identification is a continuous process within the organization.

Step 3. Create and update controls.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
Goal 3: Control designs are analyzed to ensure they satisfy control objectives.	
2. As a result of the controls analysis, are new controls introduced or existing controls modified to address gaps? [CTRL:SG3.SP1]	PR.IP-7: Protection processes are continuously improved.

Once the organization has identified and documented the control gaps, it can improve the controls, either by updating existing controls or proposing new controls to address the gaps found in Step 2.

Updating Existing Controls

In some cases, an organization will find a gap in a particular control, and it may need to be slightly updated or redesigned. As technologies change and new processes are introduced, the existing controls need to evolve. The example in Table 6 demonstrates a service-level control objective, the gaps in its associated controls, and the updates to the controls.

Table 6: Example Updates to Existing Controls

Service-Level Control Objective	Existing Service Controls	Gap	Proposed Updates to the Existing Controls
Access to the network and any network-connected system (e.g., file and print services, application servers, database servers) is controlled to prevent access by unauthorized entities.	System owner grants network access to staff based on approved access request forms.	Resource limitations or constraints	Change the implemented manual process to an automated process that requires fewer resources.
	Annually, IT personnel verify the current network/system access list with system owners to ensure network/system access is appropriate and accurate.	Insufficient period of review for controls in place	Periodically (monthly), IT managers verify the current network/system access list with system owners to ensure network/system access is appropriate and accurate.
	Administrative access, enabling the administrator to grant network/system access, is restricted to IT personnel.	Lack of adequate supporting processes	Administrative access, enabling the administrator to grant network/system access, is restricted to IT managers.

In the example above, an analysis of the service-level controls was conducted. It was determined that the current controls addressing the responsibility for verifying and granting network/system access were not applied at the appropriate level, and that reviews were not conducted with an adequate frequency. The update to the controls consisted of targeting the correct personnel and updating the frequency at which the activity is conducted.

Proposing New Controls

In addition to updating existing controls, new controls can be introduced or layered with existing controls to help satisfy one or more control objectives. When implementing new controls, organizations should consider a defense-in-depth approach. Defense in depth will help ensure that the failure of any one control will not result in the complete failure of the associated control objective. New controls can also be in the form of compensating controls or “helper” controls that would help to contain or minimize the failure of a control.

Defense in depth is an approach to security in which multiple levels of security and methods are deployed to guard against failure of one component or levels. See Section IV, Step 2 for a more detailed explanation.

When suggesting new controls, an organization should carefully consider the costs and resources required to implement them. By utilizing the defense-in-depth methodology, an organization can minimize costs by focusing on the outer layers of defense, which are inherited by all internal layers. A link to the risk management process should be established to ensure that the new control is properly evaluated on how it could affect the organization.

See the Risk Management Resource Guide, Volume 7 of this series. Also see the Risk Management (RISK) process area in the CERT-RMM for additional information on managing risks.

The example in Table 7 illustrates the proposal of a new control to compensate for an existing control. The new compensating control provides a new level of supervision.

Table 7: Example New Control Proposal

Service-Level Control Objective	Service Controls	Gap	Proposed Compensating or “Helper” Control
Access to the network and any network-connected system (e.g., file and print services, application servers, database servers) is controlled to prevent access by unauthorized entities.	System owner grants network access to staff based on approved access request forms.	Lack of adequate supporting processes	All access request forms will be reviewed and approved by the supervisor of the staff member before transmittal to the system owner.

Control layering is different from control redundancy. An organization will want to avoid deploying redundant controls, or deploying the same type of controls that will satisfy the same control objectives, which can become costly.

Step 4. Establish linkages to the risk management process.

The analysis process will enable the organization to recognize risks that were not readily apparent while selecting the controls. The personnel performing the controls management analysis should be well versed in the risk management process. During this step, the organization should document residual risks or new risks that arise when a control cannot fully satisfy control objectives. These risks should then be communicated to stakeholders and fed into the risk management process.

Utilizing the risk management process will allow the organization to properly manage these new and residual risks according to established risk thresholds. The following is a list of risk areas for the organization to consider during this step:

- risks related to unsatisfied control objectives—The control objective prioritization list can facilitate how the risk will be managed (i.e., higher priority control objectives are handled first).

- risks related to redundant controls—These risk most often lead to unnecessary expenses.
- risks related to conflicting controls—These risks often lead to a decrease of operational resilience.
- risks related to changing regulatory guidance—Changing regulation can introduce changes in guidance or new controls into the control catalog. The organization should consider the risks of these changes.

See the Risk Management Resource Guide, Volume 7 of this series. Also see the Risk Management (RISK) process area in the CERT-RMM for additional information on managing risks.

Step 5. Update security requirements traceability matrix.

Throughout the analysis process, the organization should document any changes to the control within the SRTM. As discussed in the previous steps, gaps and risks will be identified. New controls or updates to existing controls are introduced. It is important to update the matrix with these changes. This matrix will be the starting point from which the organization will periodically review the effectiveness of controls.

As a result of this step, the SRTM should be updated to include the items shown in the columns of Table 8. The information outlined in Steps 2-4 above should be added to the Control Gap and the Proposed Existing/New Control columns of the SRTM.

Table 8: Example SRTM Updates

Control Type	Control Objectives	Control Activity	Control Testing Procedures	Authority	Control Gap	Proposed Existing/New Control
Technical	Access enforcement	Determine if the information system enforces approved authorizations for logical access to the system in accordance with applicable policy.	Examine the access control policy and procedures addressing access enforcement and create a procedure to test the automated mechanisms implementing access enforcement policy.	NIST Special Publication 800-53A, Revision 1: Guide for Assessing the Security Controls in Federal Information Systems and Organizations	Lack of adequate infrastructure or supporting processes and technology	Update access enforcement policy to require user access to be reviewed every 30 days. Update infrastructure to support a single sign-on implementation.

Step 6. Deploy controls.

As the analysis is completed, the organization will begin to deploy controls. The analysis conducted in the previous steps should give the organization a high degree of confidence that the defined controls will satisfy the objectives. Once controls are deployed, the organization needs to determine the frequency at which the controls should be assessed, as described in the next section. Different personnel within the organization will be responsible for deploying controls of different levels (i.e., enterprise, service, or asset), as in the following example:

- enterprise-level controls—corporate IT, human resources department
- service-level controls—business unit manager, service delivery manager
- asset-level controls—network engineer, system administrator

Outputs of Section V

	Output	Guidance
✓	Analysis results	Analysis method will utilize subjective and formal tests and define control gaps
✓	Control gaps	List of control gaps where the organization's control objectives are not fully satisfied
✓	Updates to existing controls	Updated controls based on the results of the analysis
✓	Proposed new controls	New controls based on the results of the analysis
✓	Risks related to unsatisfied control objectives and redundant and conflicting controls	New risks identified during the analysis process that should be fed into the organization's risk management process for further action
✓	Control objectives that are satisfied by controls	After the above steps are complete and the analysis process satisfactorily addressed, the organization will have a high degree of confidence that control objectives are satisfactorily achieved by the controls selected.
✓	Updated security requirements traceability matrix	An updated SRTM, either in database or spreadsheet form, that captures the results of the analysis process
✓	Controls implemented within the organization	At the completion of the analysis process, the organization will begin deploying the controls.



VI. Assess Controls

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 assessing the controls.

	Input	Guidance
✓	Controls deployed in the internal control system	The controls the organization has deployed to meet its resilience requirements
✓	Security requirements traceability matrix	An up-to-date SRTM listing the organization's controls objectives and the controls to satisfy those objectives.

Step 1. Staff the assessment process and identify stakeholders.

For the assessment process to be successful, it must be conducted by the appropriate personnel, and key stakeholders will need to be notified of the impending assessment on the internal control system.

Key personnel performing the assessment should have the following responsibilities:

- developing the assessment process and scope
- analyzing and assessing the controls
- managing internal/external entities during the assessment process
- summarizing the assessment results

Stakeholders include

- owners of enterprise-level controls such as policies and procedures
- service/asset owners
- compliance officer responsible for regulatory activities
- those responsible for executing controls
- external entities such as regulators, auditors, and service providers

Depending on the scope of the assessment, specialized training may be required for the personnel performing the assessment or the stakeholders supporting it.

See the Training and Awareness Resource Guide, Volume 9 of this series. Also see the Organizational Training and Awareness (OTA) process area in the CERT-RMM for additional information on managing an effective training program and setting training requirements.

Step 2. Establish a schedule.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
Goal 4: The internal control system is assessed to ensure control objectives are met.	
1. Is the performance of controls assessed on a scheduled basis to verify they continue to meet control objectives? [CTRL:SG4.SP1]	PR.IP-7: Protection processes are continuously improved.

Once the organization has implemented its control management plan, it must periodically assess the controls that have been put into place. This assessment should focus on the effectiveness of controls, be ongoing, and be used to improve operational resilience enabling action on its results.

Setting the Schedule

Each organization will have to set the time table for assessments. Inputs for consideration are

- high-value controls objectives
- high-value services
- high-value assets
- significant changes to operating environment

See the Asset Management Resource Guide, Volume 1 of this series. Also see the Asset Definition and Management (ADM) process area in the CERT-RMM for additional information on managing and defining high-value assets and services they support.

System Development Lifecycle

The organization may also want to consider conducting assessments according to the five generic system development lifecycle phases:

- initiation
- development/acquisition
- implementation
- operations and maintenance
- disposal

An organization utilizing this method would schedule an assessment at the beginning of each of the phases of the system development lifecycle. The results of the first assessment should be included in the next assessment's scope to ensure action was taken.

NIST Special Publication 800-53A, Chapter 2, provides more detailed guidance for organizations using this method and overall guidance for establishing an assessment process.

Linkage to the Vulnerability Management Process Area

An organization should also consider linking the controls assessment process to its vulnerability management program. As vulnerabilities are discovered in information, people, technology, and facility assets, the organization should consider scheduling assessments to ensure that the vulnerability did not affect the asset's ability to meet control objectives and resilience requirements.

See the Vulnerability Management Resource Guide, Volume 4 of this series. Also see the Vulnerability Analysis and Resolution (VAR) process area in the CERT-RMM for additional information on managing vulnerabilities to assets.

Step 3. Define the scope.

It is important for the organization to choose a well-defined scope when assessing controls. Assessments at various levels of the organization should be considered, and each assessment should have a clearly defined scope. Depending on the size of the service under assessment, the organization may want to conduct a series of assessments that would focus on subsystems and the high-value assets (people, technology, information, and facilities) that support that service. The organization should ensure that the chosen assessments collectively meet the organization’s risk management needs.

The scope of the assessment should focus on the controls the organization has deployed to support the operational resilience of that service, with the objective of identifying deficiencies and remediating them. The example in Table 9 highlights an example of a high-value service, its scope, and a breakdown of manageable assessments.

Table 9: Example Assessment Scope

High-Value Service	Scoping Statement	Assessments
Electricity generation	The scope of this assessment will be the organization’s ability to generate electricity at Facility A and the service’s related assets.	<ul style="list-style-type: none"> • <u>Assessment 1</u>: Facility A control room (<i>technology asset</i>) • <u>Assessment 2</u>: Facility A SCADA system (<i>technology asset</i>) • <u>Assessment 3</u>: Configuration management system (<i>information assets/technology assets</i>) • <u>Assessment 4</u>: Training program effectiveness (<i>people asset/enterprise control</i>)

Step 4. Perform the assessment.

After the organization has determined the scope of the assessment, it can start to perform assessment activities.

Methods of Assessment

Assessments can be performed in a variety of ways including but not limited to those in Table 10.

Table 10: Assessment Methods

Assessment Type	Pros	Cons
Self-assessments	<ul style="list-style-type: none"> • Inside knowledge • Not resource intensive 	<ul style="list-style-type: none"> • Potentially biased
Interviews	<ul style="list-style-type: none"> • Direct feedback • Ability to inquire further 	<ul style="list-style-type: none"> • Time consuming • Can be costly
Surveys	<ul style="list-style-type: none"> • Quick • Can reach the masses 	<ul style="list-style-type: none"> • Not all data received will be useful
Internal assessment standard	<ul style="list-style-type: none"> • Specifically tailored to organization 	<ul style="list-style-type: none"> • Requires specially trained individual • May not scale to all services and assets
Business impact analysis	<ul style="list-style-type: none"> • Provides prioritized list of organization’s most important services 	<ul style="list-style-type: none"> • Resource intensive
External audits	<ul style="list-style-type: none"> • Independent entity performing the assessment • Provides outside perspective 	<ul style="list-style-type: none"> • Can be costly

Automated assessments	<ul style="list-style-type: none"> • Regular reporting • Cost efficient over the long haul 	<ul style="list-style-type: none"> • Resource intensive for deployment
-----------------------	--	---

When selecting a method for performing the assessment, it is important for the organization to recognize that the assessment process is an information-gathering process. The assessments allow the organization to measure the effectiveness of implemented controls that will ultimately work to achieve the control objectives on an ongoing basis.

Identify Problem Areas

During the performance of assessments, assessors should be looking for and documenting the problem areas in Table 11. The table’s example controls are for illustration only and may not represent a problem area in all organizations.

Table 11: Problem Areas for Consideration

Potential Problem Area	Example
Ineffective control	A hashing algorithm that can be easily defeated is implemented in the infrastructure.
Inefficient control	A gate is implemented with no other detective or preventive controls in place (i.e., cameras or guards).
Redundant control	A room of IT cabinets has 24/7 camera recording access <i>and</i> alarms that are recorded when a cabinet door is open.
Conflicting control	Enterprise- and system-level password requirements conflict.

Leverage Existing Assessment Results

Assessments should also leverage existing documentation from other process areas such as the results of service continuity exercises, incident handling responses, and risk assessments. Looking back on existing documentation from these areas could give the organization useful insight on how control objectives have been satisfied or have failed.

See the Service Continuity Resource Guide, Volume 6 of this series. Also see the Service Continuity (SC) process area in the CERT-RMM for additional information on conducting service continuity exercises.

See the Incident Management Resource Guide, Volume 5 of this series. Also see the Incident Management and Control process area in the CERT-RMM for additional information on handling incidents.

See the Risk Management Resource Guide, Volume 7 of this series. Also see the Risk Management process area in the CERT-RMM for additional information on managing risks.

Step 5. Improve the process.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
Goal 4: The internal control system is assessed to ensure control objectives are met.	
2. As a result of scheduled assessments, are new controls introduced or existing controls modified to address problem areas? [CTRL:SG4.SP1]	PR.IP-7: Protection processes are continuously improved

The results of a completed assessment will enable the organization to make informed decisions to improve the controls management plans and strategies. Once the organization has identified the problem areas, it can begin to identify updates to existing controls and propose new controls. These updates or new controls are typically performed by either the service or asset owners.

Refer to Section V, Step 3 of this Resource Guide for information on updating and proposing new controls.

The organization will also identify new risks associated with the problem areas discovered during the assessment. These risks should be documented in accordance with the organization's risk management process, and any risks not fully resolved should be included in the scope of the service's or asset's next assessment.

Refer to Section V, Step 4 of this Resource Guide for information on documenting new risks resulting from the controls management process.

When problem areas are broad and encompass changes to organizational processes and procedures, a remediation plan may be needed. Below is a list of considerations to be included in a remediation plan:³⁰

- actions the organization must take to ensure that controls satisfy control objectives effectively and efficiently
- changes to the internal control system
- assignment of responsibility and authority to perform the work
- schedule and resources required to perform the work
- documentation of risk mitigation strategies and residual risks

Feedback Loop

As depicted in Figure 1, the assessment of controls and control objectives is an ongoing process for the organization. As technology and processes changes, so must the internal control system. These changes should always be assessed so that decisions related to the operational resilience of the organization can be properly managed.

The organization should leverage other process areas during the feedback loop. Lessons learned from the deployment of other processes may yield controls that will enable the organization to increase its operational resilience. Process areas to consider include the following:

- **Asset Management**—The organization may decide on a more efficient means of commissioning and decommissioning technology assets. The controls necessary to realize these efficiencies should be fed into the controls management process.
- **Incident Management**—As incidents are investigated, breakdowns of the internal control system will become known. These breakdowns should be discussed during the post-incident brief, and recommendations to improve the controls management process should be made.
- **Risk Management**—The organization's normal risk review sessions will reveal new risks. The revealed risks that can be mitigated by controls should be fed into the controls management plan.
- **Service Continuity**—As disaster recovery and business continuity plans are developed and exercised, failures should be documented and recommendations for new control objectives and controls should be fed into the controls management process.

The list above provides examples for the organization to consider. Process areas not listed have an opportunity to provide inputs to the controls management plan as well.

KEY TAKEAWAY: *The organization should always look to improve its operational resilience by leveraging other process areas and the outputs they provide.*

Step 6. Update control objectives and controls.

The final step in the assessment process enables the organization to implement the updates and new controls. The process outlined above provides the due diligence an organization needs to confidently assess the internal control system and make changes based on the assessment.

As updates are made, it is important for the organization to schedule follow-on reassessments to ensure that the updates and new controls are effectively achieving control objectives.

Output of Section VI

	Output	Guidance
✓	Assessment report	Assessment report that outlines the areas below
✓	Control gaps	List of control gaps where the organization's control objectives are not fully satisfied
✓	Updates to existing controls	Updated controls based on the results of the assessment
✓	Proposed new controls	New controls based on the results of the assessment
✓	Risks related to unsatisfied control objectives and redundant and conflicting controls	Residual risks identified during the assessment process that should be fed into the organization's risk management process for further action
✓	Remediation plans	Plans that will ensure control objectives are satisfactorily addressed
✓	Updated SRTM	An updated traceability matrix, either in database or spreadsheet form, that captures the results of the assessment process



VII. Conclusion

Establishing and supporting an ongoing controls management program enables your organization to evaluate the effectiveness of the internal control system that protects the people, information, technology, and facilities of the organization. The controls management program helps to ensure that your organization can sustain its critical services and meet its responsibility to its stakeholders and its contribution to national critical infrastructure.

The following documents provide broad program guidance:

- *NIST Special Publication SP 800-53* (<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>) provides a catalog of controls for information systems.
- *NIST Special Publication SP 800-53A* (<http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf>) provides guidelines for conducting assessments on information systems.
- The *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 the website of the Office of Cybersecurity and Communications at <http://www.dhs.gov/office-cybersecurity-and-communications>.

Appendix A. Security Requirements Traceability Matrix Template

Control Type	Control Objectives	Control Activity	Control Testing Procedures	Authority	Control Gap	Proposed Existing/New Control
Technical	Access Enforcement	Determine if the information system enforces approved authorizations for logical access to the system in accordance with applicable policy.	Examine the access control policy and procedures addressing access enforcement and create a procedure to test the automated mechanisms implementing access enforcement policy.	NIST Special Publication 800-53A, Revision 1: <i>Guide for Assessing the Security Controls in Federal Information Systems and Organizations</i>	Lack of adequate infrastructure or supporting processes and technology	Update access enforcement policy to require user access to be reviewed every 30 days. Update infrastructure to support a single sign-on implementation.

Appendix B. Controls Management Resources

Information Systems Audit and Control Association (ISACA)

<http://www.isaca.org>

- Control Objectives for Information and Related Technology (COBIT)
<http://www.isaca.org/COBIT/Pages/default.aspx>

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/>
 - NIST Special Publication 800-53, *Recommended Security and Privacy Controls for Federal Information Systems and Organizations*
 - NIST Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*
 - NIST Special Publication 800-82, *Guide to Industrial Control Systems (ICS) Security*
 - NIST Special Publication 800-115, *Technical Guide to Information Security Testing and Assessment*

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

<http://www.ics-cert.us-cert.gov>

- Catalog of Control Systems Security: Recommendations for Standards Developers, April 2011, U.S. Department of Homeland Security National Cybersecurity and Communications Integration Center, ICS-CERT.
<http://ics-cert.us-cert.gov/sites/default/files/documents/CatalogofRecommendationsVer7.pdf>
- Cyber Security Procurement Language for Control Systems, U.S. Department of Homeland Security National Cyber Security Division, September 2009.
http://ics-cert.us-cert.gov/sites/default/files/documents/Procurement_Language_Rev4_100809.pdf

Software Engineering Institute, CERT Division

<http://www.sei.cmu.edu/>

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

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

Table 12 cross-references CRR Controls 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.

Domain goals and practice questions to the sections of this guide that address those questions.

Table 12: Cross-Reference of CRR Goals/Practices and NIST CSF Categories/Subcategories Against the Controls Management Resource Guide

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory	Controls Management Resource Guide Reference
Goal 1: Control objectives are established.		
1. Have control objectives been established for assets required for delivery of the critical service? [CTRL:SG1.SP1]	<p>ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.</p> <p>PR.AC: Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.</p> <p>PR.DS: Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.</p> <p>PR.IP: Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.</p> <p>PR.MA: Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.</p> <p>PR.PT: Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.</p>	Section III, Step 2
2. Are control objectives prioritized according to their potential to affect the critical service? [CTRL:SG1.SP1]	<p>ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.</p> <p>PR.AC: Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.</p> <p>PR.DS: Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.</p> <p>PR.IP: Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.</p> <p>PR.MA: Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.</p> <p>PR.PT: Technical security solutions are managed to ensure the security and resilience of systems and assets,</p>	Section III, Step 2

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory	Controls Management Resource Guide Reference
	consistent with related policies, procedures, and agreements.	
Goal 2: Controls are implemented.		—
1. Have controls been implemented to achieve the control objectives established for the critical service? [CTRL:SG2.SP1]	<p>ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.</p> <p>PR.AC: Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.</p> <p>PR.DS: Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.</p> <p>PR.IP: Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.</p> <p>PR.MA: Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.</p> <p>PR.PT: Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.</p>	Section IV, Steps 1 and 2
Goal 3: Control designs are analyzed to ensure they satisfy control objectives.		—
1. Are control designs analyzed to identify gaps where control objectives are not adequately satisfied? [CTRL:SG3.SP1]	PR.IP-7: Protection processes are continuously improved.	Section V, Step 2
2. As a result of the controls analysis, are new controls introduced or existing controls modified to address gaps? [CTRL:SG3.SP1]	PR.IP-7: Protection processes are continuously improved.	Section V, Step 3
Goal 4: The internal control system is assessed to ensure control objectives are met.		—
1. Is the performance of controls assessed on a scheduled basis to verify they continue to meet control objectives? [CTRL:SG4.SP1]	PR.IP-7: Protection processes are continuously improved.	Section VI, Step 2
2. As a result of scheduled assessments, are new controls introduced or existing controls modified to address problem areas? [CTRL:SG4.SP1]	PR.IP-7: Protection processes are continuously improved.	Section VI, Step 5

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®-RMM: 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. The *CERT-RMM* (CTRL:SG1) [Caralli 2010] discusses control objectives.
5. The *CERT-RMM* (Glossary of Terms) [Caralli 2010]
6. The *CERT-RMM* (EF:SG1) [Caralli 2010] discusses the need for resilience activities to meet strategic objectives.
7. Gates, L.P., *Strategic Planning with Critical Success Factors and Future Scenarios: An Integrated Strategic Planning Framework* [CERT 2010], discusses strategic planning.
8. Gates, L.P., *Strategic Planning with Critical Success Factors and Future Scenarios: An Integrated Strategic Planning Framework* [CERT 2010], discusses strategic planning.
9. The *CERT-RMM* (CTRL:SG1) [Caralli 2010] discusses how to identify management directives and organizational guidelines.
10. The *CERT-RMM* (CTRL:SG1) [Caralli 2010] discusses how to identify management directives and organizational guidelines.
11. COBIT [The IT Governance Institute, 2007] discusses the requirements for control objectives.
12. The *CERT-RMM* (CTRL:SG1:SP1) [Caralli 2010] discusses prioritizing control objectives.
13. The *CERT-RMM* (ADM:SG1:SP1) [Caralli 2010] discusses inventory of high-value assets.
14. The *CERT-RMM* (EF:SG1:SP3) [Caralli 2010] discusses inventory of high-value services.
15. The *CERT-RMM* (CTRL:SG2) [Caralli 2010] discusses administrative controls.
16. The *CERT-RMM* (CTRL:SG2) [Caralli 2010] discusses administrative controls.
17. FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems* [NIST 2006], defines “technical control.”
18. COBIT [The IT Governance Institute, 2007] discusses IT general controls and application controls.
19. COBIT [The IT Governance Institute, 2007] discusses IT general controls and application controls.
20. The *CERT-RMM* (CTRL:SG3:SP1) [Caralli 2010] discusses a controls analysis process.
21. The *CERT-RMM* (CTRL:SG2) [Caralli 2010] discusses the internal control process.
22. The *CERT-RMM* (CTRL:SG2) [Caralli 2010] discusses enterprise-level controls.
23. COBIT [The IT Governance Institute, 2007] discusses enterprise-level controls.
24. The *CERT-RMM* (CTRL:SG2:SP1) [Caralli 2010] discusses service-level controls.
25. The *CERT-RMM* (CTRL:SG2:SP1) [Caralli 2010] discusses service- and asset-level controls.
26. The *CERT-RMM* (CTRL:SG2:SP1) [Caralli 2010] discusses asset-level controls.

27. The *CERT-RMM* (CTRL:SG2) [Caralli 2010] discusses layering of controls.
28. May, C.J., Hammerstein, J., Mattson, J., and Rush, K., *Defense in Depth: Foundations for Secure and Resilient IT Enterprises* [CERT 2006], discusses defense-in-depth.
29. The *CERT-RMM* (CTRL:SG3.SP1) [Caralli 2010] discusses control gaps.
30. The *CERT-RMM* (CTRL:SG4.SP1) [Caralli 2010] discusses remediation plans.