CRR Supplemental Resource Guide

Volume 1

Asset Management

Version 1.1

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

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.

DM-0003275

Table of Contents

I. Introduction

Series Welcome

Welcome to the CRR Supplemental Resource Guide series! This document was developed by the Department of Homeland Security's (DHS) Cyber Security Evaluation Program (CSEP). It is the first of 10 resource guides intended 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* for IT operations. Operational resilience indicates 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 as well as times of operational stress and crisis. The guides were developed for organizations that have participated in a CRR, but are useful to any organization interested in implementing or maturing operational resilience capabilities for critical IT services.

The 10 domains covered by the CRR Resource Guide series are

1. Asset Management ⇦***This guide***

2. Controls Management
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. Be aware 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 either fall short of or exceed the corresponding practices and capabilities in the NIST CSF.

Each resource guide in this series has the same basic structure but 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 make use of complementary materials and suggestions to optimize their adoption approach. For example, this Asset Management guide outlines how to identify and document critical assets, which can then be used as the basis for identifying controls according to the Controls 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 an asset management process. To outline this process, this document will use an approach common to many asset management standards and guidelines. The process areas described include

- planning for asset management
- identifying the assets
- documenting the assets
- managing the assets

More specifically this guide

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

The guide is structured as follows:

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

II. Asset Management—Presents an overview of the asset management process and establishes some basic terminology.

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

III. Plan for Asset Management—Highlights the elements necessary for an effective asset management plan.

IV. Identify the Assets—Presents a process for identifying assets based on asset type.

V. Document the Assets—Provides an approach for documenting assets.

VI. Manage the Assets—Outlines a process for managing assets within the organization.

VII. Conclusion—Provides contacts and references for further information.

Appendices

A. Asset Profile Catalog
B. Service Catalog
C. Asset Management Resources
D. 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 asset 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 organizational assets.

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

II. Asset Management

Overview

Asset management establishes an organization’s inventory of high-value assets and defines how these assets are managed during their lifecycle to ensure sustained productivity in support of the organization’s critical services. The CRR defines four broad categories of assets: people, information, technology, and facilities. An event that disrupts an asset can inhibit the organization from achieving its mission. An asset management program helps identify appropriate strategies that will allow the assets to maintain productivity during disruptive events.

The Asset Management domain focuses on the processes by which an organization plans, identifies, documents, and manages the assets within the organization. The process depicted in Figure 1 helps the organization ensure the asset management objectives are satisfied.

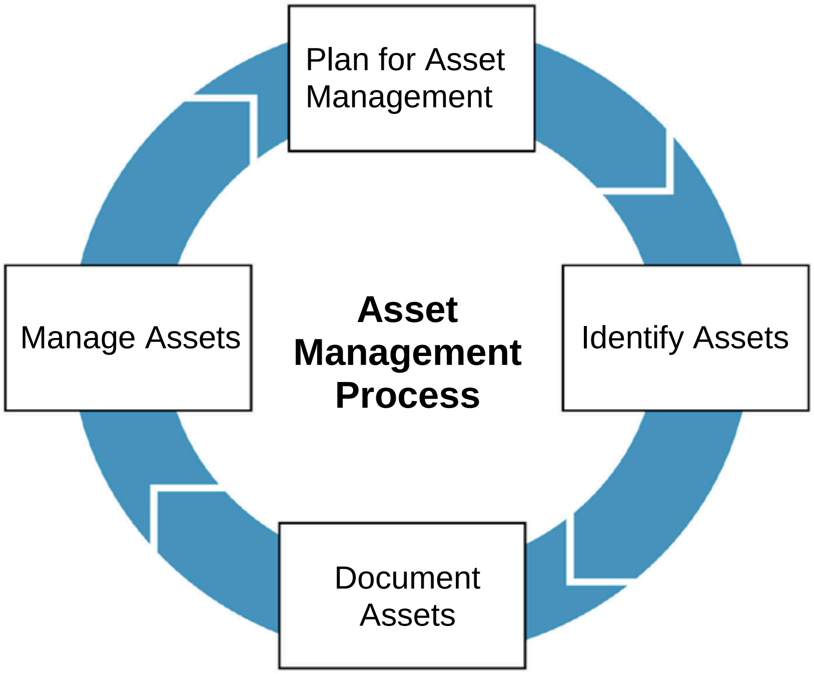


Figure 1: The Asset Management Process

This guide focuses on defining how assets are related to the services that allow an organization to achieve its mission. An organization’s assets require various levels of management and staff to plan, identify, document, and manage. 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 Asset Management

Asset management gives an organization a snapshot of all the assets within the infrastructure at any given time. Developing and following a plan is essential to efficient and effective asset management. Planning for asset management includes obtaining support from higher level management to ensure that the process is funded, staffed, and performed. Key activities include identifying all the mission-critical services the organization performs or provides and prioritizing them according to their potential to disrupt operations should they fail. The organization can then focus its resources to appropriately protect and sustain its assets. Finally, planning for asset management requires the organization to establish a common definition of what constitutes an asset within its infrastructure.

Important activities while planning for asset management covered in this guide include the following:

- Obtain support for asset management planning.
- Identify services.
- Prioritize services.
- Establish a common definition of assets.

*A **service** is a set of activities that the organization carries out in the performance of a duty or in the production of a product.*[4]

Identify the Assets

A key component of this effort involves identifying the critical services and the assets that support them. Responsibility for this effort should be delegated to a level appropriate for the critical service being considered. This guide organizes assets into the following categories: people, information, technology, and facilities. It is important to note that these assets may be internal to the organization or reside within a business partner or other external entity.

Important activities while identifying assets include the following:

- Assign responsibility for identifying assets supporting critical services.
- Identify people assets.
- Identify information assets.
- Identify technology assets.
- Identify facility assets.

Document the Assets

Once these assets have been identified, it is important to document them in order to understand their relationship to the organization (e.g., internal, external), who is responsible for the asset, how well the asset is protected from disruption, how important the asset is to the critical service, and any changes or updates that may affect the asset throughout its lifecycle.

This documentation typically includes the following:

- asset type (people, information, technology, or facilities)
- categorization of asset by sensitivity (generally for information assets only)
- asset location (typically where the custodian is managing the asset)
- asset owners and custodians (especially if assets are external to the organization)

- format or form of the asset (particularly for information assets that might exist on paper or electronically)
- location of asset backups or duplicates (particularly for information assets)
- services that are dependent on the asset[5]
- value of the asset, either qualitative or quantitative
- asset protection and sustainment requirements

Important activities while documenting assets include the following:

- Create an asset inventory.
- Document the relationships between assets and critical services.
- Analyze dependencies between assets supporting multiple services.
- Update the asset inventory.

Manage the Assets

The organization will need to manage its assets and inventories and takes steps to improve the process of asset management. The organization should select tools and methods (configuration databases, drawings, change control) to manage the assets and also determine how these tools are applied within.

Important activities in the asset management process include the following:

- Identify change criteria.
- Establish a change schedule.
- Manage changes to assets and inventory.
- Update asset inventory when changes occur.
- Improve the process.

Summary of Steps

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

Plan for Asset Management

1. Obtain support for asset management planning.
2. Identify services.
3. Prioritize services.
4. Establish a common definition of assets.

Identify the Assets

1. Assign responsibility for identifying assets supporting critical services.
2. Identify people assets.
3. Identify information assets.
4. Identify technology assets.
5. Identify facility assets.

Document the Assets

1. Create an asset inventory.
2. Document the relationships between assets and critical services.

3. Analyze dependencies between assets supporting multiple services.
4. Update the asset inventory.

Manage the Assets

1. Identify change criteria.
2. Establish a change schedule.
3. Manage changes to assets and inventory.
4. Update asset inventory when changes occur.
5. Improve the process.

Organizations that already have an asset management program can assess and improve it by using the guidance in this Resource Guide.

III. Plan for Asset 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 an asset management program.

	Input	Guidance
✓	Scoping statement	This statement defines what the asset management program and plan need to address. Asset management should cover, at a minimum, all assets that support 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. If your organization has participated in a CRR, it may be beneficial to begin with the critical service addressed during the CRR. See Appendix D 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 • 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 an asset management program and implementing processes
✓	An understanding and acknowledgement of an acceptable approach to asset management	Acceptance from management for the intended approach to asset management, including stakeholder expectations about acceptable risk tolerance for the identified critical assets and services
✓	Externally imposed requirements for asset management	Regulatory requirements defining mandatory requirements for asset definition; also includes other needs such as service-level agreement requirements
✓	Risks	The list of categorized and prioritized risks
✓	Assignment of responsibility for asset management	Job descriptions for roles that have responsibilities for asset management, for example, executive ownership, decisions, communication, testing, and disruption risk management
✓	Budget for asset management	Identification of available funds to perform asset management planning and execution, including • staffing resources • tools (applications and associated hardware) • third-party support • funding to correct asset management issues identified by the asset management process

Step 1. Obtain support for asset management planning.

Obtaining support from management is essential to ensuring that the asset management plan is effectively implemented. A top-down approach often helps the asset management program meet the resilience objectives of the organization. Management can demonstrate support by providing appropriate funding, oversight, and staffing. A top-down approach also enables a consistent methodology for asset management to be implemented across organizational boundaries.

The level of management support required depends on where assets reside within the organization. For an asset management plan that addresses the entire organization, support at the senior executive level is necessary. Smaller implementations, such as those at the service level, may only require sponsorship from the management responsible for that particular service. For example, consider an electric utility that has four business units providing the following services: generation, transmission, distribution, and business support. An asset management program could be implemented for these services individually with sponsorship coming from management for that business unit. Alternatively, senior management of the electric utility could require a common asset management program for all business units.

Step 2. Identify services.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
Goal 1: Services are identified and prioritized.	
1. Are services identified? [SC:SG2.SP1]	ID.BE: The organization’s mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.

Identifying assets within an organization can be a daunting task, so the organization should first identify the services it provides. It can then identify assets by the services they support and divide the body of assets into manageable pieces.

Services are defined as the limited number of activities that the organization carries out in the performance of a duty or in the production of a product.[6] Services typically will align with a particular organization, but a service can be shared between business units and cross organizational boundaries. For example, a large organization’s global supply chain will cross many organizational boundaries. Possible sources of helpful information in determining an organization’s services include

- strategic plans
- business plans
- contracts
- customer requests
- standard work processes

Services can be both externally and internally focused. Externally focused services are typically customer facing and are often the easiest services to identify because they involve a known commodity. For the external services to achieve their missions, the organization should also consider its internal services (hiring processes, performance reviews, training programs, etc.). Table 1 highlights different critical infrastructure organizations and services they may provide.

Table 1: Organizations and Example Critical Services

Organization	Critical Service
Electric Utility	Generation of electricity Human resources (hiring qualified personnel)
Bank	Loan processing for consumers Online banking
Hospital	Emergency medical services Advanced medical research
Communications Utility	Provide cable, telephony, and internet service Technician training program

To facilitate the work done during this step of the process, the organization should consider a method of documentation to keep track of the identified services. This can include documenting in a spreadsheet, a configuration-controlled document, or a database. Appendix B provides an example of a service catalog in spreadsheet form and the data an organization may want to capture. Each organization will have to determine which tool best suits its needs. Documentation of assets is discussed further in Section V of this document.

KEY CONCEPTS:

External Services*—services that are often customer facing and focus on specific products an organization produces or supports*

Internal Service*—departments, teams, processes, etc. that support the internal organizational units and allow the organization to achieve its mission*

Step 3. Prioritize services.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
Goal 1: Services are identified and prioritized.	
2. Are services prioritized based on analysis of the potential impact if the services are disrupted? [SC:SG2.SP1]	ID.BE: The organization’s mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions. ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value.

After the organization has identified all of the services it provides, it should then prioritize those services. High-value services are services that are critical to the success of the organization’s mission.[7] Their failure may prevent the organization from meeting strategic objectives. Figure 2 illustrates an example of how an organization’s critical service can be disrupted, whether due to failures in processes or through failures of specific assets such as information or technology.

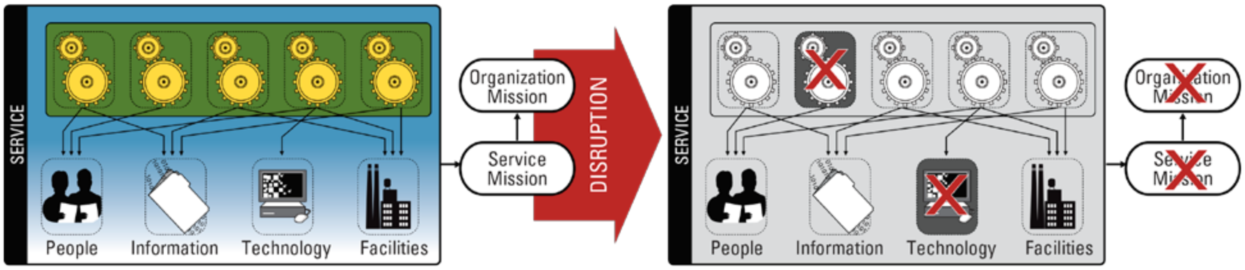


Figure 2: Failure of Critical Service

The organization must decide how to assign value to its own services. When assigning value and prioritizing services, the organization should consider the following:

- results from a business impacts analysis (BIA)
- service/business continuity plans
- consequences of risks to services identified during risk assessment activities
- strategic objectives
- safety classification

Once the organization has prioritized its services, it should document this information in the documentation tool selected in the previous step.

By properly prioritizing services, an organization can proportionately allocate budget and resources for resilience activities with the services that matter most, such as identifying assets.

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 identifying high-value services.

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 to services.

Step 4. Establish a common definition of assets.

After the organization develops an understanding of the services that are required to achieve its mission, it needs to define an understanding of the assets that support those services. Assets are the raw materials that services need in order to operate.[8,9] A service needs

- people
- information
- technology
- facilities

People

People assets are the vital staff who operate and monitor the organization's services. People who are internal to the organization (and sometimes people who are external) are in charge of executing processes and procedures to ensure that the services are achieving the organization's mission. Table 2 lists examples of internal and external people assets for different kinds of organizations.

Table 2: Example Internal and External People Assets

Organization	Internal People Asset	External People Asset
Electric utility	Industrial control system engineer Technician	Equipment manufacturer support team
Bank	Teller Loan officer	Compliance auditor
Hospital	Doctor Lab technician	IT help desk
Communications utility	Service request coordinator Network engineer	Contracted technician

When identifying people assets, the organization should consider the vital role required for the successful operation of a service rather than the actual person in that role. It is suggested that each role contain a defined list of the functions or responsibilities required in the performance of that role.

Defining the functions for each role will help the organization ensure that personnel are sufficiently skilled to carry out that role and that more than one person can support the role. It also helps identify training needs when deficiencies in personnel are found. See the Training and Awareness Resource Guide, Volume 9 of this series, for additional information on identifying and documenting training deficiencies.

Information

Information assets are any information or data, on any media, required for the successful operation of an organizational service. An information asset can also be the output or by-product of a service. Table 3 lists examples of information assets within different kinds of organizations.

Table 3: Example Common Information Assets

Organization	Information Asset Required for Successful Service Operation	Information Asset Created as an Output to a Service
Electric utility	Control system set points	Grid vulnerability report
Bank	List of loan types available to consumers	Loan records
Hospital	Vaccination research methodology	Vaccination structure (intellectual property)
Communications utility	Service packages	Network maps of where service is located

Information can range from a bit or byte, a file, or a document, to the collective information stored in a database. The organization must determine the granularity with which it wants to define its information assets.

Technology

Technology assets include software, hardware, firmware, and any physical interconnections. Technology assets can reside anywhere within an organization, and it is up to the organization to determine how it describes the technology assets. A good starting point would be at the network-device level, where common network components such as routers, servers, and switches can be identified. The organization could then move on to the personal computing devices such as PCs, laptops, and tablets. Identifying broad categories gives the organization a starting point for uniquely identifying all of the devices within its infrastructure as well as set boundaries for controls management.

See the Controls Management Resource Guide, Volume 2 of this series. Also see the Controls Management (CTRL) process area in the CERT-RMM for more detailed guidance on how to identify controls for assets.

Facilities

Facility assets are any physical plant an organization relies on when delivering or performing a service. Facilities can be owned and controlled by the organization or be under the control of external business partners. Table 4 contains examples of facility assets both internal and external to different kinds of organizations.

Table 4: Example Common Facility Assets

Organization	Internal Facility Asset	External Facility Asset
Electric Utility	Power plant	Partner electric distribution facility
Bank	Headquarters building	Credit union office

Organization	Internal Facility Asset	External Facility Asset
Hospital	Walk-in care office	Research lab
Communications utility	Central office	Maintenance vehicle garage

Facility assets house the people, technology, and information assets discussed previously, and the protection strategies for all the assets must be integrated.

Output of Section III

	Output	Guidance
✓	Prioritized list of services	A prioritized list that clearly identifies the highest valued services
✓	Asset definitions	Assets are clearly defined for the organization so that the stakeholders responsible for identifying assets can consistently document them.

IV. Identify the Assets

Before You Begin

The following checklist summarizes the tasks you will need to complete and the information you will need to gather before you can begin identifying assets.

	Input	Guidance
✓	Prioritized list of services	A prioritized list that clearly identifies the highest valued services
✓	Asset definitions	Assets are clearly defined for the organization so that the stakeholders responsible for identifying assets can consistently document them
✓	An understanding and acknowledgement of an acceptable approach to asset management	Acknowledgement from management for the intended approach to asset management, including stakeholder expectations about acceptable risk tolerance for the identified critical assets and services
✓	Externally imposed requirements for asset management	Regulatory requirements defining mandatory requirements for asset definition; also includes other needs such as service-level agreement requirements
✓	Risks	The list of categorized and prioritized risks
✓	Assignment of responsibility for asset management	Job descriptions for roles that have responsibilities for asset management, for example, executive ownership, decisions, communication, testing, and disruption risk management

Step 1. Assign responsibility for identifying assets that support critical services.

Identifying key stakeholders for each component of a critical service is essential to understand how the organization approaches service design. These stakeholders often support multiple services within an organization and can offer unique insights on the assets involved in supporting them. A typical organization will have individuals serving in work roles (outlined in Table 5), whether through a formal assignment process or, in smaller organizations, informally based on traditionally performed work roles.

The relationships between these individuals and each asset type can be further illustrated using a Responsible, Accountable, Consulted, Informed (RACI) Matrix.[10] A responsible role manages the asset on a day-to-day basis. An accountable role has to answer to higher level management when issues arise with that asset. A consulted role has specific knowledge of the asset or relies on that asset and needs to provide input. An informed role would need to be updated on the activities surrounding that asset. Table 5 shows an example of this concept.

Table 5: Example RACI Matrix

Work Role	Typical Position Within the Organization	Asset Type: People	Asset Type: Information	Asset Type: Technology	Asset Type: Facilities
Executive sponsor	EVP / VP / director-level sponsor	Accountable	Informed	Informed	Informed
Service design manager	Chief technology officer / architect	Responsible	Responsible	Responsible	Consulted
Project manager	Project manager / Project analyst	Informed	Informed	Informed	Informed
Service delivery manager (business process owner)	Functional manager / information technology manager	Responsible	Accountable	Accountable	Consulted
Service developers (internal or external)	Information technology analysts / business analysts (may include external contractors)	Consulted	Consulted	Responsible	Consulted
Operational technology engineers implementation	Operational technology engineer / operators (may include external contractors)	Consulted	Consulted	Consulted	Consulted
Quality assurance	Sr. information technology analysts / business analysts	Consulted	Consulted	Responsible	Informed

These key stakeholders should be able to identify and inventory the assets of the organization. This inventory will often include

- asset owners
- asset custodian
- asset profiles that contain
  - process mapping, service-level agreements (with internal or external customers)
  - mandated policy
  - regulatory or legal framework imposed on the service
  - inventory of the supporting information technology and operational technology systems
  - understanding of key personnel and internal teams involved in the support of the service
  - external contracts or supplier dependencies

A discussion on establishing ownership (accountability) and custodianship (responsibility) for each asset can be found in the CERT-RMM description of Asset Definition and Management.[11]

Asset Owner—A person or organizational unit, internal or external to the organization, that has primary responsibility for the viability, productivity, and resilience of an organizational asset.[12]

Asset Custodian—A person or organizational unit, internal or external to the organization, responsible for satisfying the resilience requirements of a high-value asset while it is in the custodian's care.[13]

Step 2. Identify people assets.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
Goal 6: Information assets are categorized and managed to ensure the sustainment and protection of the critical service.	
4. Are all staff members who handle information assets (including those who are external to the organization, such as contractors) trained in the use of information categories? [KIM:SG1.SP2]	PR.AT-1: All users are informed and trained.

Organizations rely on the experience, talents, and capabilities of internal (and in many cases, external) people to support critical services. Employees are key to an organization's success. They are responsible for executing the organization's mission and are a key component in its ability to adapt to change or disruption and remain resilient. Focusing on an employee's work role allows an organization to capture the critical knowledge, skills, and abilities required for the position.

Individuals responsible for identifying people assets should consider interfacing with the following groups and people within the organization:

- human resources department—provides demographic information, which can underlie a base profile of the individuals currently serving in those work roles
- supervisors, managers, and directors—provide an assessment of how well an individual currently performs a specific work role and help tailor the profile to capture the specific background of employees who have been successful within that role
- people external to the organization—provide information on their roles that support a critical service, to ensure a complete picture of the requirements for that service

As people assets are identified, information about those assets will need to be collected. Table 6 shows examples of the types of information that should be included when identifying people assets.

Table 6: Examples of People Asset Information

Work Role	Level of Experience Required (Apprentice, Journeyman, Master) or Years' Experience	Educational Qualifications	Required Knowledge	Required Skills	Required Abilities	Certification / Licensure
Service design manager	Journeyman/master 8–10 years exp.	B.S. in CS or related field; masters preferred	SDLC,[a] ITSM,[b] Agile	.Net multi-tier development, source code control	Technical documentation	ITIL[c] v3
Project manager	Journeyman/master 8–10 years exp.	B.S. in engineering, business, management; masters pref.	Critical path mapping	Microsoft Project	Project budgeting, resource tracking	PMP[d]
Service developers (internal or external)	Apprentice, journeyman 3–5 years exp.	B.S. in CS or related field	SDLC, Agile	.Net multi-tier development	Technical documentation	MCPD[e]

[a] system development lifecycle

[b] information technology service management

[c] Information Technology Infrastructure Library
[d] Project Management Professional
[e] Microsoft Certified Professional Developer

Step 3. Identify information assets.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
Goal 5: Access to assets is managed.	
1. Is access to assets granted based on their protection requirements? [AM:SG1.SP1]	PR.AC-1: Identities and credentials are managed for authorized devices and users. PR.AC-2: Physical access to assets is managed and protected. PR.AC-3: Remote access is managed.
2. Are access requests reviewed and approved by the asset owner? [AM:SG1.SP1]	PR.AC-1: Identities and credentials are managed for authorized devices and users. PR.AC-2: Physical access to assets is managed and protected. PR.AC-3: Remote access is managed.
3. Are access privileges reviewed to identify excessive or inappropriate privileges? [AM:SG1.SP3]	PR.AC: Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.
4. Are access privileges modified as a result of reviews? [AM:SG1.SP3]	PR.AC: Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.
Goal 6: Information assets are categorized and managed to ensure the sustainment and protection of the critical service.	
1. Are information assets categorized based on sensitivity and potential impact to the critical service (such as public, internal use only, secret)? [KIM:SG1.SP2]	PR.DS: Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.
2. Is the categorization of information assets monitored and enforced? [KIM:SG1.SP2]	PR.DS: Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.

Information assets must be carefully mapped to each critical service. This information may include not only the technical documentation involved in supporting the service, but also the actual information contained within the database or record structure itself. Information assets to consider also include

- key configuration requirements for supporting systems (e.g., identity and access management permissions, DNS entries)
- periodic batch processes that must be run to maintain peak performance
- back-up scripts that provide snapshots of the critical information
- proprietary algorithms developed internally that provide unique capability for the organization
- software licensing and purchasing documentation
- vendor support agreements and the people authorized to contact the vendor
- access requirements for each information asset

Information must be able to be found, opened, used, understood, and trusted in order to be of value to the organization.[14]

A data custodian should be assigned to each critical service to ensure this information is appropriately inventoried, cataloged, and archived in accordance with the organization’s policies and any regulatory or legal compliance requirements. Information within an organization may be bound by retention requirements that must be carefully monitored to ensure that only the essential information required for the execution of that critical service is maintained for the specified timeline. Keeping too much or too little information introduces additional risk to the organization that must be avoided. Keeping too much information ties up resources and adds cost to the overall operation. Keeping too little information may open the organization to a variety of fines or other punitive measures as spelled out under an applicable regulatory regime.

The data custodian must also ensure that appropriate controls are enacted to protect the information assets of the critical service. Enterprise- and service-level controls should be defined, implemented, and assessed to ensure that the appropriate level of confidentiality, integrity, and availability of the information assets are maintained.[15] The organization's policies should clearly spell out these controls.

At all times, a data custodian should know exactly who has access to the types of information under the custodian's purview. This access should be periodically reviewed by internal audit or an independent organization to ensure compliance with stated policy and with legal and regulatory requirements. All changes to the access level of an individual must be formally documented and approved.

Organizations should consider implementing access control measures to protect their information assets. Access control models include

- identity-based access control (IBAC)
- role-based access control (RBAC)
- attribute-based access control (ABAC)

ABAC is typically more ideal for information assets where "distinguishable characteristics of users or resources, conditions defined by an authority, or aspects of the environment, and policies specify how to use attributes to determine whether to grant or deny an access request."[16]

Figure 3 illustrates a model for identity and access management. It includes example activities for provisioning, administering, and enforcing user access to information.[17]

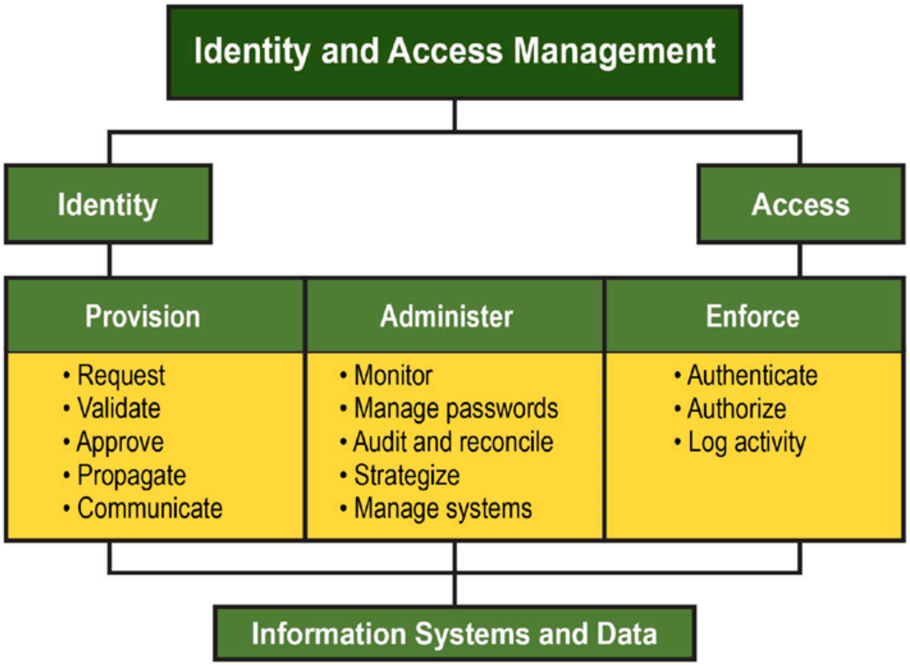


Figure 3: Identity and Access Management Model

Step 4. Identify technology assets.

Technology assets must be evaluated in terms of their relationship to a critical service. This evaluation will often focus on the application layer, but the underlying components and their interdependencies must be carefully considered.

The technology assets should include all components involved in delivering or supporting a critical service, whether a traditional information technology asset or an operational technology asset. Identifying the systems on which a critical service relies is essential to understanding the service's resilience posture.

The architecture of a critical service and the technology assets supporting it can be illustrated using a layered approach. For instance, the remote terminal units that support environmental monitoring at a wastewater treatment facility may include telemetry sensors. The organization may not identify these sensors as assets at first, but the layered view of the service and asset architecture makes it obvious that these sensors are important to the function of the top-layer asset (remote terminal unit). Figure 4 depicts this concept.

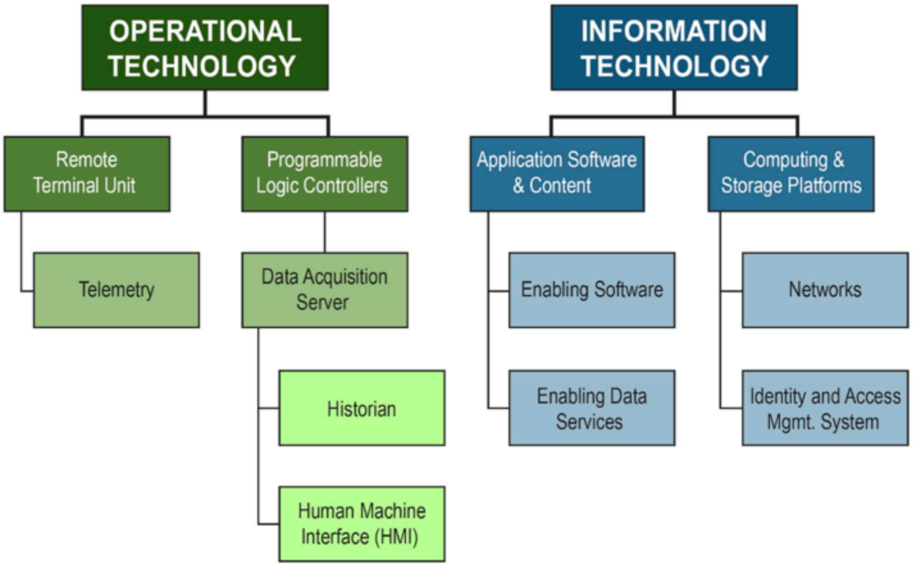


Figure 4: Layered Illustration of Critical Service Architecture and Supporting Technology Assets

Each of these components should be included in an enterprise configuration management database and managed through formal change control processes as described in Section VI of this document.

Step 5. Identify facility assets.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
Goal 7: Facility assets supporting the critical service are prioritized and managed.	
1. Are facilities prioritized based on potential impact to the critical service, to identify those that should be the focus of protection and sustainment activities? [EC:SG1.SP1]	ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value. ID.BE-4: Dependencies and critical functions for delivery of critical services are established.
2. Is the prioritization of facilities reviewed and validated? [EC:SG1.SP1]	ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value.

	ID.BE-4: Dependencies and critical functions for delivery of critical services are established.
3. Are protection and sustainment requirements of the critical service considered during the selection of facilities? [EC:SG2.SP2]	ID.BE-5: Resilience requirements to support delivery of critical services are established.
	PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met.

Critical services rely on the people, information, and technology to support customer requirements, either internally to the organization or as an external supporting element. Each of these assets requires a physical facility in which to execute this service. The facilities involved in supporting this effort may be shared across multiple services, and ownership may be distributed across many organizations.

As the facility assets are identified, the organization should be cognizant of how that facility affects the services it performs. The organization should prioritize the facilities so that it can focus resources on the facilities that affect the critical services first. This prioritization should be periodically reviewed and updated on a schedule determined by the organization.

It is essential to identify the primary owner and custodian for the facility assets involved in supporting a critical service. The responsibility for a facility asset may not fall under a traditional operational department and may be considered an ancillary service to the organization. In planning for resilience, it is important to document the facility assets and help highlight their involvement in supporting the critical service. When designing their services, key stakeholders may not have considered the importance of the infrastructure or facilities. The organization should ensure that its resilience requirements will be met by any new facilities.

Output of Section IV

	Output	Guidance
✓	RACI matrix by asset	A Responsible, Accountable, Consulted, Informed (RACI) matrix of each work role by asset allows organizations to assign the appropriate level of oversight to each asset and track other areas of the organization that need to be included in discussions about the asset itself.
✓	List of assets by type and service	A comprehensive list of the assets, by type, involved in supporting a specific critical service is essential to documenting the assets' lifecycles and roles in the organization.

V. Document the Assets

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 to document assets.

	Input	Guidance
✓	Prioritized list of services	A prioritized list that clearly identifies the highest valued services
✓	Asset definitions	Assets are clearly defined for the organization so that the stakeholders responsible for identifying assets can consistently document them.
✓	An understanding and acknowledgement of an acceptable approach to asset management	Acknowledgement from management for the intended approach to asset management, including stakeholder expectations about acceptable risk tolerance for the identified critical assets and services
✓	Externally imposed requirements for asset management	Regulatory requirements defining mandatory requirements for asset definition; also includes other needs such as service-level agreement requirements
✓	Risks	The list of categorized and prioritized risks
✓	RACI matrix by asset	A Responsible, Accountable, Consulted, Informed (RACI) matrix of each work role by asset allows organizations to assign the appropriate level of oversight to each asset and track other areas of the organization that need to be included in discussions about the asset itself.
✓	List of assets by type and services	A comprehensive list of the assets, by type, involved in supporting a specific critical service is essential to documenting the assets' lifecycles and roles in the organization.

Step 1. Create an asset inventory.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
1. Are the assets that directly support the critical service inventoried? [ADM:SG1.SP1]	ID.AM: The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy. ID.AM-1: Physical devices and systems within the organization are inventoried. ID.AM-2: Software platforms and applications within the organization are inventoried. ID.AM-4: External information systems are catalogued.
2. Do asset descriptions include protection and sustainment requirements? [ADM:SG1.SP2]	ID.BE-5: Resilience requirements to support delivery of critical services are established.
3. Are both owners and custodians of assets documented in asset descriptions? [ADM:SG1.SP3]	ID.AM: The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.

4. Are the physical locations of assets (both within and outside the organization) documented in the asset inventory? [ADM:SG1.SP3]	ID.AM: The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.

A standardized inventory of the organization's assets should be created based on the list of critical services and the assets that support them, identified in Section IV. This inventory typically contains an asset profile that includes the following types of information:[18]

- asset type (people, information, technology, or facilities)
- categorization of asset by sensitivity (generally for information assets only)
- asset location (typically where the custodian is managing the asset)
- asset owners and custodians (especially if assets are external to the organization)
- format or form of the asset (particularly for information assets that might exist on paper or electronically)
- location of asset backups or duplicates (particularly for information assets)
- services that are dependent on the asset[19]
- value of the asset, either qualitative or quantitative
- asset protection and sustainment requirements

This list of information types is not exhaustive. The organization should take the time to define the right level information to document for their assets. Appendix A contains an asset profile template that an organization can use as a starting point.

Step 2. Document the relationships between assets and critical services.

Once the inventory with asset profiles is established, the organization should document the relationships between assets and the services they support. Within the inventory, each asset profile should be updated with all of the services that the asset supports, enabling the organization to see what assets support multiple services.

One method for documenting the assets involved in supporting critical services is identified in *NIST Interagency Report 7693, Specification for Asset Identification 1.1*.[20] This specification presents an overview of asset management and guidelines for asset identification using an extensible markup language (XML) schema. The specification gives examples of how an organization can use identifiers within a database to identify assets and relationships. For example, a literal identifier can be used to track MAC addresses or the real name of a people asset. A synthetic identifier is assigned by the organization and is often used to identify people assets, as with employee identification numbers. Finally, the specification discusses relationship identifiers, so that an asset may be identified based on its relationships to other assets. These relationship identifiers can be a simple designation of "INTERNAL" or "EXTERNAL" or something as complex as a business unit or critical service function.

Step 3. Analyze dependencies between assets supporting multiple services.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
Goal 3: The relationship between assets and the services they support is established.	
1. Are the associations between assets and the critical service they support documented? [ADM:SG2.SP1]	ID.BE-4: Dependencies and critical functions for delivery of critical services are established.

2. Are confidentiality, integrity, and availability requirements established for each service-related asset? [RRD:SG2.SP1]	ID.BE-5: Resilience requirements to support delivery of critical services are established. ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.

When an organization examines its resiliency, it should carefully consider the interdependencies between assets that support multiple critical services. Documenting the assets and relationships as described above provides an organization with a baseline for considering whether resilience requirements have been implemented at an appropriate level for each asset.

The critical service inventory (with relationships identified as in Step 2) can help an organization analyze and reveal dependencies between assets and services within an organization. It also allows assets to be grouped in many ways, such as by service domains, service types, and service components. Analysis of these dependencies and the potential overlap between assets (e.g., facilities used to support multiple services) can help organizations identify assets of significance whose confidentiality, integrity, or availability should be carefully considered.

For instance, an organization depends on both service A and service B to achieve its mission. Service B contains more stringent requirements for its assets than service A. The results of a dependency analysis show that many assets support both service A and service B. If the organization is not aware that the assets support both services, the assets may only receive the less stringent requirements of service A, which could expose the assets to disruption in ways unacceptable to service B.

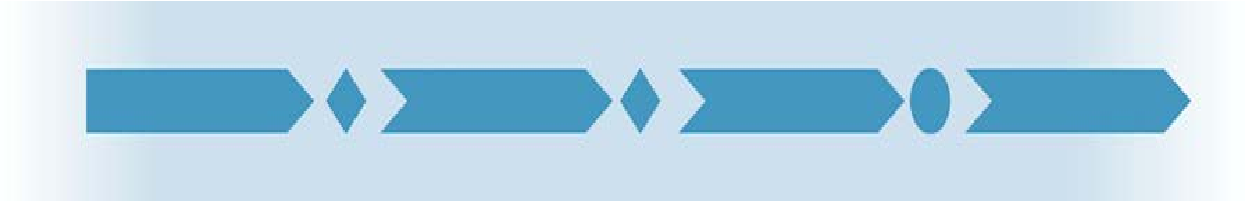
Step 4. Update the asset inventory.

To support its services, an organization should have a configuration management database (CMDB) that can be repeatedly revised to provide more comprehensive asset management. Configuration management can often be the foundation for broader service management and facilitate management of the lifecycle of those services and their related assets. It is important to track and document any changes or updates to an asset throughout its lifecycle, keeping in mind potential impacts to the broader service the asset supports.

See the Configuration and Change Management Resource Guide, Volume 3 of this series, for more detailed guidance on establishing a configuration and change management program.

Output of Section V

	Output	Guidance
✓	Service-asset analysis	A mapping of the critical services and their supporting assets can help illustrate overlap and dependencies within the organization.
✓	Asset profile	A robust asset profile will provide the organization with a thorough understanding of the asset itself, its ability to respond to disruption, and any changes made throughout its lifecycle.
✓	Configuration management database (CMDB)	A formal CMDB that can be repeatedly revised to provide more comprehensive asset management.



VI. Manage the Assets

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 selecting methods of managing the assets.

	Input	Guidance
✓	Identified assets	Before the organization can manage its assets, the people, technology, information, and facilities of the organization must be identified.
✓	Identified owners and custodians of the assets	Asset owners and custodians are identified to support the management of the assets.
✓	Asset documentation	Documentation of the assets should exist, clearly identifying the services they support.
✓	Configuration management database (CMDB)	A formal CMDB that can be repeatedly revised to provide more comprehensive asset management.

Step 1. Identify change criteria.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
Goal 4: The asset inventory is managed.	
1. Have change criteria been established for asset descriptions? [ADM:SG3.SP1]	ID.AM: The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.

Organizational assets are dynamic. As assets change, their resilience requirements and protection strategies change as well. For the organization to effectively manage its assets, it must actively monitor for changes that significantly alter assets, identify new assets, or call for the retirement of assets for which there is no longer a need.[21]

To make it easier to evaluate changes to assets, develop a set of change criteria that is consistently applied within the organization. The change criteria should cover all of the asset types: technology, people, information, and facilities. Through the effective use of change criteria, changes within assets can be translated into changes in the resilience requirements. Table 7 illustrates change criteria that an organization might implement.

Table 7: Example Change Criteria for Assets

Asset Type*	Change Criteria
People	Changes in organizational structure and staff
Technology	Changes in technology infrastructure or configuration

Asset Type*	Change Criteria
Facilities	Real estate transactions that add, alter, or change existing facilities
Information	Creation or alteration of information
P, T, I, F	Changes in services affecting the assets on which they rely
T, F, I	An asset entering or exiting a phase of the system development lifecycle
T, F	Acquisition of assets such as technology or facilities

* P = people, T = technology, F = facility, I = information

To illustrate this point further, consider electric utility A which has just acquired smaller utility B in its service area. Changes in the organizational structure will occur to ensure that utility B's organizational structure aligns with the mission of utility A. This will require the people in utility B to receive specialized training. Utility B also introduced new facilities to utility A, and resilience requirements such as security practices will be need to be implemented at those facilities. Having identified change criteria will greatly assist the new organization identify and track changes to its asset inventory and ensure that resilience requirements are captured.

Document Change Criteria

To ensure that change criteria are consistently applied, even in times of organizational stress, official documentation should be created in the form of policy and procedures. Typical documentation can include

- field change procedures—used when making changes during implementation phases
- engineering change notice procedures—used when making changes during design phases
- change control board procedures—roles and responsibilities of personnel that approve/disapprove changes resulting from field changes and engineering changes

Step 2. Establish a change schedule.

Link Asset Management to the System Development Lifecycle

A schedule for updating assets and reviewing resilience requirements can be a useful tool for managing changes. As a starting point, an organization may consider linking the review of technology, information, and facility assets to the system development lifecycle (SDLC). Figure 5 depicts the SDLC as presented in NIST SP 800-64.[22]

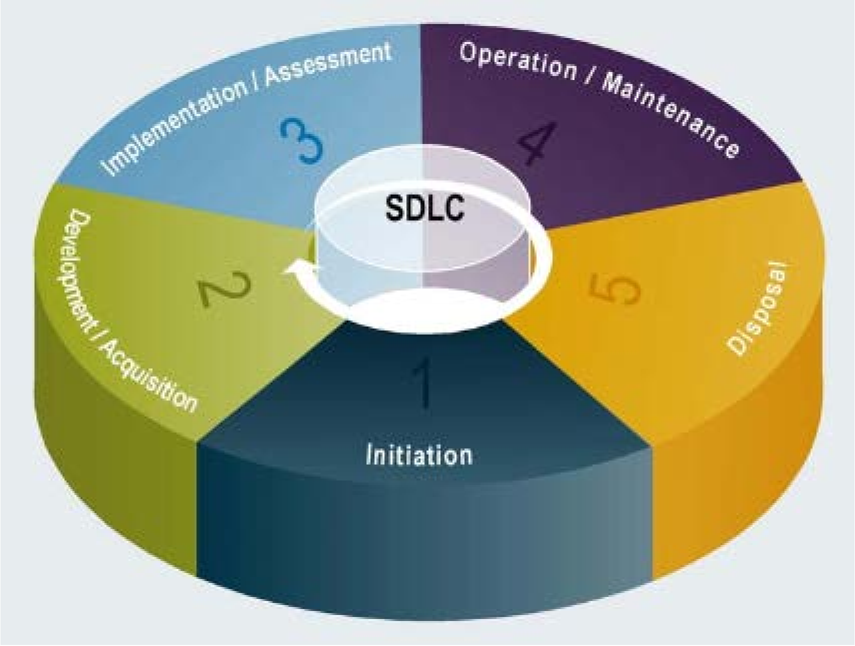


Figure 5: System Development Lifecycle

Linking asset management to the SDLC can provide many benefits, such as

- a means to identify milestones for an asset (e.g., software testing completion, facility upgrade)
- early identification of potential vulnerabilities in assets
- awareness of potential challenges in the assets as the designs are reviewed
- documentation of resilience decisions for each SDLC phase

The SDLC approach can also be adopted for use in other CRR domains such as Controls Management. See the Controls Management Resource Guide, Volume 2 of this series. Also see the Controls Management (CTRL) process area in the CERT-RMM for more detailed guidance on how to identify controls.

Implement a Change Schedule for People Assets

Scheduled changes to people assets require a different approach because the concepts in the SDLC generally do not scale. Common tools like performance reviews can be used to document the skills of personnel and identify training needs. The organization should determine the frequency at which these reviews should take place.

Implement a Change Schedule for Information, Technology, and Facility Assets

Regardless of the asset type in need of review, the organization should determine the frequency for this activity. The frequency can be dictated by the organization's management or through documentation such as assessment procedures.

Step 3. Manage changes to assets and inventory.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
Goal 6: Information assets are categorized and managed to ensure the sustainment and protection of the critical service.	
3. Are there policies and procedures for the proper labeling and handling of information assets? [KIM:SG1.SP2]	PR.DS: Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
6. Do guidelines exist for properly disposing of information assets? [KIM:SG4.SP3]	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition. PR.IP-6: Data is destroyed according to policy.
7. Is adherence to information asset disposal guidelines monitored and enforced? [KIM:SG4.SP3]	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition. PR.IP-6: Data is destroyed according to policy.

As change criteria are defined and implemented, the organization should develop methods for managing changes to its assets. An organization will typically have many methods for managing and documenting assets. This documentation can be in the form of drawings, organizational charts, or procedures. The following sections will outline the different asset types and possible solutions for managing them.

Manage People Assets

Staffs change in many ways, including adding new staff members (internally or externally), transferring staff from one organizational unit to another, and terminating staff. Table 8 highlights various tools an organization can use to manage its people assets.

Table 8: Tools for Managing People Assets

Tool	Benefit
Organization chart	• Ease of maintenance • Pictorial representation of where people assets reside
Performance review	• Scheduled review • Skill gaps can be identified, addressed, and documented
Succession planning	• Develops people assets to be future leaders of the organization
Title and associated job descriptions	• Clearly defines specific roles • Facilitates performance reviews
Exit interview	• Provides insight on improvements than can be made within the organization to retain people assets

Manage Information Assets

Changes to information include the creation, alteration, or deletion of paper and electronic records, files, and databases. Table 9 highlights various tools an organization can use to manage its information assets.

Table 9: Tools for Managing Information Assets

Tool	Benefit
Document database	• Information stored in a central location • Can be configuration controlled
Information disposal policy	• Provides clear expectations for disposal of information
Employing a numbering system	• Uniquely identifies information • Version can be tracked by revision level
Information sensitivity levels	• Ensures the handling of information at varying sensitivity levels

Manage Technology Assets

Changes to technology include refreshes, addition of new technical components, changes to existing technical components, and the elimination or retirement of existing technology. Table 10 highlights various tools that an organization can use to manage its technology assets.

Table 10: Tools for Managing Technology Assets

Tool	Benefit
Technology refresh program	• Ensures organization's technology remains current
Configuration baselines	• Ensures rapid deployment of technology should an asset fail
Asset database	• Enables organization to uniquely identify, locate, and document its technology assets
Network map	• Provides snapshots of what is connected to the network • Helps asset owners and custodians determine relationships between assets

Manage Facility Assets

Changes to facilities include the addition of new facilities (owned by the organization or external business partner), alteration of existing facilities, and the retirement of a facility. Table 11 highlights various tools an organization can use to manage its facility assets.

Table 11: Tools for Managing Facility Assets

Tool	Benefit
As-built drawings	• Graphically depict current configurations within the facility
Preventive maintenance schedule	• Ensures that the facility infrastructure is maintained on a consistent basis, extending its life to support the service
Asset database	• Enables organization to uniquely identify, locate, and document its facility assets

Step 4. Update asset inventory when changes occur.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
Goal 4: The asset inventory is managed.	
2. Are asset descriptions updated when changes to assets occur? [ADM:SG3.SP2]	ID.AM: The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.

After the organization determines which tools to use for managing its assets, it should focus on keeping the asset inventory current. A current asset inventory is critical to ensuring that high-value services achieve their missions.

To keep asset inventories current, the organization should regularly update the following types of documentation when changes occur:

- asset documentation
- asset profiles
- asset inventory status
- asset and service resilience requirements
- asset and service protection strategies and controls
- strategies and continuity plans for sustaining assets and services

Implementing proper configuration control on the assets is a useful way for the organization to establish the documentation needed along with the history of changes to the assets.

For information regarding configuration management of assets, see the Configuration and Change Management Resource Guide, Volume 3 of this series.

Step 5. Improve the process.

As shown in Figure 1, asset management is an ongoing process for the organization. As the organization's services evolve and technology and processes change, so must the assets that support those services. The organization should continually assess these changes to properly manage decisions related to operational resilience.

The organization should leverage other CRR domains to improve asset management. Lessons learned from the deployment or management of assets in different parts of the organization may provide information that will enable the organization to manage those assets uniformly. CRR domains to consider include the following:

- Controls Management—The organization may decide to use different security controls to commission and decommission technology assets more efficiently. The controls necessary to realize these efficiencies should be fed into the asset management process so assets that support these controls can be implemented.
- Incident Management—The assets compromised during an incident should be discussed during the post-incident brief. Recommendations to improve the management of the assets should be made.
- Risk Management—The organization's normal risk review sessions will reveal new risks, which might be mitigated by feeding them into the asset management program.
- Service Continuity—As disaster recovery and business continuity plans are developed and exercised, failures should be documented and recommendations for new assets should be fed into the asset management program.

The list above provides examples for the organization to consider. CRR domains not listed may also have a bearing on the asset management plan.

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

Outputs of Section VI

	Output	Guidance
✓	Documented change criteria	Change criteria utilized within the organization to facilitate the evaluation of changes to assets.
✓	Schedules	Scheduled activities to assess assets to ensure they are supporting their service's mission.
✓	Asset management tools	The organization should have a defined set of tools and techniques to manage the assets within the organization.
✓	Updated asset inventories	Updated asset descriptions and inventories utilizing the criteria and tools discussed in this section.

VII. Conclusion

Establishing and supporting an ongoing asset management program enables an organization to effectively manage the many people, information, technology, and facility assets contained within the organization's infrastructure. The asset management program helps ensure that your organization can sustain its critical services, meet its responsibility to its stakeholders, and make its contribution to national critical infrastructure.

The following resources provide broad program guidance:

- *The IT Infrastructure Library* (http://www.itil-officialsite.com/) provides guidance on implementing an asset management program.
- 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 http://www.us-cert.gov/ccubedvp/self-service-crr.

Appendix A. Asset Profile Catalog

Asset Profile Catalog (Critical Services)

Number of Assets

People: __________

Information: __________

Technology: __________

Facilities: __________

Total Assets: __________

Total number of assets defined: __________

Total number of assets supporting critical services: __________

Total number of assets supporting ancillary services: __________

Date the asset profile catalog was last reviewed: __________

ID **(unique)**	**Name** **(unique)**	**Services Supported (service IDs)**	**Type** *People* *Information* *Technology* *Facility*	**Location**	**Owner**	**Custodian**	**Format** (e.g., *paper, electronic, tape*)	**Security Classification** *SBU* *Confidential* *Secret* *Top Secret* *TS-SCI*	**Backup/DR Locations**	**Business Impact of Disruption (Asset Value)** *0*=None *2*=Minimal *4*=Moderate *6*=Moderately Heavy *8*=Heavy *10*=Severe				
										Loss of Revenue	**Additional Expenses**	**Regulatory & Legal**	**Customer Service**	**Goodwill**

Appendix B. Service Catalog

Critical Service Catalog Component Definition List (Service Name)

Service catalog entries defined: _________

SLA or OLA documented: _________

Metrics defined for the service: _________

BC/DR plan has been documented: _________

Service cost model developed: _________

Communications distribution list identified: _________

Number of critical services defined: _________

Number of other types of services defined: _________

Total number of services defined: _________

Date the service catalog was last reviewed: __________

ID (unique)	Name (unique)	Portfolio	Information Technology (ownership)	Operational Technology (ownership)	Functional Owner (dept.)	SC Entry Defined?	SLA/OLA Defined?	Metrics Defined?	BC/DR Defined?	Cost Model	Dist. List	Service Category		Average Users	Potential Users	Business Impact of Disruption (Asset Value) *0*=none *2*=minimal *4*=moderate *6*=moderately heavy *8*=heavy *10*=severe				
												Critical: mission critical service *Direct*: direct customer support *Indirect*: secondary support *Utility*: enterprise/background	Impact *1 2 3 4 5* lo hi			Loss of Revenue	Additional Expenses	Regulatory & Legal	Customer Service	Goodwill

Appendix C. Asset Management Resources

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
http://www.ics-cert.us-cert.gov

- Rinaldi et al. "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies." *IEEE Control Systems Magazine*, 2001.
  http://www.ce.cmu.edu/~hsm/im2004/readings/CII-Rinaldi.pdf

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

Information Technology Infrastructure Library (ITIL)
http://www.itil-officialsite.com/Publications/Publications.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 800-64, *Security Considerations in the Information System Development Life Cycle*
  - NIST Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*

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

Table 12 cross-references the CRR Asset Management Domain goals and practice questions to the NIST CSF Categories/Subcategories and the sections of this guide that address those questions. Users of this guide may wish to review the CRR Question Set with Guidance available at https://www.us-cert.gov/ccubedvp for more information on interpreting practice questions. The NIST CSF, available at https://www.us-cert.gov/ccubedvp also provides informative references for interpreting Category and Subcategory statements.

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

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/ Subcategory	Asset Management Resource Guide Reference
Goal 1: Services are identified and prioritized.		
1. Are services identified? [SC:SG2.SP1]	ID.BE: The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	Section III, Step 2
2. Are services prioritized based on analysis of the potential impact if the services are disrupted? [SC:SG2.SP1]	ID.BE: The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions. ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value.	Section III, Step 3
Goal 2: Assets are inventoried, and the authority and responsibility for these assets is established.		—
1. Are the assets that directly support the critical service inventoried? [ADM:SG1.SP1]	ID.AM: The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy. ID.AM-1: Physical devices and systems within the organization are inventoried. ID.AM-2: Software platforms and applications within the organization are inventoried. ID.AM-4: External information systems are catalogued.	Section V, Step 1
2. Do asset descriptions include protection and sustainment requirements? [ADM:SG1.SP2]	ID.BE-5: Resilience requirements to support delivery of critical services are established.	Section V, Step 1
3. Are both owners and custodians of assets documented in asset descriptions? [ADM:SG1.SP3]	ID.AM: The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	Section V, Step 1
4. Are the physical locations of assets (both within and outside the organization) documented in the asset inventory? [ADM:SG1.SP3]	ID.AM: The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	Section V, Step 1

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/ Subcategory	Asset Management Resource Guide Reference
Goal 3: The relationship between assets and the services they support is established.		—
1. Are the associations between assets and the critical service they support documented? [ADM:SG2.SP1]	ID.BE-4: Dependencies and critical functions for delivery of critical services are established.	Section V, Step 3
2. Are confidentiality, integrity, and availability requirements established for each service-related asset? [RRD:SG2.SP1]	ID.BE-5: Resilience requirements to support delivery of critical services are established. ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.	Section V, Step 3
Goal 4: The asset inventory is managed.		—
1. Have change criteria been established for asset descriptions? [ADM:SG3.SP1]	ID.AM: The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	Section VI, Step 1
2. Are asset descriptions updated when changes to assets occur? [ADM:SG3.SP2]	ID.AM: The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	Section VI, Step 4
Goal 5: Access to assets is managed.		—
1. Is access to assets granted based on their protection requirements? [AM:SG1.SP1]	PR.AC-1: Identities and credentials are managed for authorized devices and users. PR.AC-2: Physical access to assets is managed and protected. PR.AC-3: Remote access is managed.	Section IV, Step 3
2. Are access requests reviewed and approved by the asset owner? [AM:SG1.SP1]	PR.AC-1: Identities and credentials are managed for authorized devices and users. PR.AC-2: Physical access to assets is managed and protected. PR.AC-3: Remote access is managed.	Section IV, Step 3
3. Are access privileges reviewed to identify excessive or inappropriate privileges? [AM:SG1.SP3]	PR.AC: Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	Section IV, Step 3
4. Are access privileges modified as a result of reviews? [AM:SG1.SP3]	PR.AC: Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	Section IV, Step 3
Goal 6: Information assets are categorized and managed to ensure the sustainment and protection of the critical service.		—
1. Are information assets categorized based on sensitivity and potential impact to the critical service (such as public, internal use only, secret)? [KIM:SG1.SP2]	PR.DS: Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	Section IV, Step 3
2. Is the categorization of information assets monitored and enforced? [KIM:SG1.SP2]	PR.DS: Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	Section IV, Step 3
3. Are there policies and procedures for the proper labeling and handling of information assets? [KIM:SG1.SP2]	PR.DS: Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	Section VI, Step 3

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/ Subcategory	Asset Management Resource Guide Reference
4. Are all staff members who handle information assets (including those who are external to the organization, such as contractors) trained in the use of information categories? [KIM:SG1.SP2]	PR.AT-1: All users are informed and trained.	Section IV, Step 2
5. Are high-value information assets backed up and retained? [KIM:SG6.SP1]	PR.IP-4: Backups of information are conducted, maintained, and tested periodically.	Section IV, Step 3
6. Do guidelines exist for properly disposing of information assets? [KIM:SG4.SP3]	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition. PR.IP-6: Data is destroyed according to policy.	Section VI, Step 3
7. Is adherence to information asset disposal guidelines monitored and enforced? [KIM:SG4.SP3]	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition. PR.IP-6: Data is destroyed according to policy.	Section VI, Step 3
Goal 7: Facility assets supporting the critical service are prioritized and managed.		—
1. Are facilities prioritized based on potential impact to the critical service, to identify those that should be the focus of protection and sustainment activities? [EC:SG1.SP1]	ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value. ID.BE-4: Dependencies and critical functions for delivery of critical services are established.	Section IV, Step 5
2. Is the prioritization of facilities reviewed and validated? [EC:SG1.SP1]	ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value. ID.BE-4: Dependencies and critical functions for delivery of critical services are established.	Section IV, Step 5
3. Are protection and sustainment requirements of the critical service considered during the selection of facilities? [EC:SG2.SP2]	ID.BE-5: Resilience requirements to support delivery of critical services are established. **PR.IP-5:** Policy and regulations regarding the physical operating environment for organizational assets are met.	Section IV, Step 5

Endnotes

1. For more information on the *Cyber Resilience Review*, please contact the Cyber Security Evaluation Program at CSE@hq.dhs.gov.
2. *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. *CERT-RMM*. "Glossary of Terms" [Caralli 2010].
5. *CERT-RMM*. "ADM:SG2, Establish the Relationship between Assets and Services" [Caralli 2010].
6. *CERT-RMM*, "ADM:SG1," discusses the role of services in an organization [Caralli 2010].
7. *CERT-RMM*, Section 2.2.1 (pg. 29), defines high-value services [Caralli 2010].
8. *CERT-RMM*. "ADM:SG1" (pg. 123) [Caralli 2010].
9. *CERT-RMM*, "ADM:SG1," defines assets as they relate to a service [Caralli 2010].
10. *ITIL Service Design, 2011 Edition*, pg. 65. The Stationery Office, 2011.
11. *CERT-RMM*. "ADM:SG1.SP3, Establish Ownership and Custodianship" [Caralli 2010].
12. *CERT-RMM*. "Glossary of Terms" [Caralli 2010].
13. *CERT-RMM*. "Glossary of Terms" [Caralli 2010].
14. *Mapping the Technical Dependencies of Information Assets*. The National Archives, v1.2, pg. 7, 2011.
15. *CERT-RMM*. "CTRL:SG2.SP1, Define Controls" [Caralli 2010].
16. *NISTIR 7657, A Report on the Privilege (Access) Management Workshop* (pg. 14). NIST/NSA Privilege Management Conference Collaboration Team, 2010.
17. "Identity and Access Management," *Global Technology Audit Guide (GTAG)* (pg. 5). The Institute of Internal Auditors (The IIA), 2007.
18. *CERT-RMM*, "ADM:SG1:SP2," outlines information to be collected for assets [Caralli 2010].
19. *CERT-RMM*. "ADM:SG2, Establish the Relationship between Assets and Services" [Caralli 2010].
20. Wunder, John; Halbardier, Adam; & Waltermire, David. *NIST Interagency Report 7693, Specification for Asset Identification 1.1* (pg. 28). National Institute of Standards and Technology.
21. *CERT-RMM*. "ADM:SG3.SP1, Identify Change Criteria" [Caralli 2010].
22. *NIST SP 800-64, Security Considerations in the System Development Life Cycle Revision 2*. NIST, 2008.