Software Engineering Institute

CERT® Resilience Management Model, Version 1.2

Resilience Requirements Development (RRD)

Richard A. Caralli
Julia H. Allen
David W. White
Lisa R. Young
Nader Mehravari
Pamela D. Curtis

February 2016

CERT Program

http://www.cert.org/resilience/

Carnegie Mellon

RESILIENCE REQUIREMENTS DEVELOPMENT

Engineering

Purpose

The purpose of Resilience Requirements Development is to identify, document, and analyze the operational resilience requirements for high-value services and related assets.

Introductory Notes

An operational resilience requirement is a characteristic, condition, or capability that must be met or possessed by an asset to ensure that it remains viable and sustainable as needed to support a service. In practice, operational resilience requirements are a derivation of the traditionally described security objectives of confidentiality, integrity, and availability. Well known as descriptive properties or quality attributes of information assets, these objectives are also extensible to other types of assets—people, technology, and facilities—with which operational resilience management is concerned.

Resilience requirements provide the foundation for protecting assets from threats and sustaining them to the extent practical and possible so that they can perform as intended in support of services. In essence, resilience requirements become a part of an asset's DNA (just like its definition, owner, and value) that transcends departmental and organizational boundaries because the requirements stay with the asset regardless of where it is deployed or operated.

Requirements drive engineering-based processes, such as operational resilience management. In operational resilience management, the Resilience Requirements Development process area requires the organization to establish resilience requirements at the enterprise, service, and asset levels. Resilience requirements also drive or influence operational resilience management process areas. For example, resilience requirements form the basis for developing protection strategies and controls and for developing sustainment and service continuity plans for services and assets.

The importance of requirements to the operational resilience management system cannot be overstated. Resilience requirements embody the strategic objectives, risk appetite, critical success factors, and operational constraints of the organization. They represent the alignment factor that ties practice-level activities performed in security and business continuity to what must be accomplished at the service and asset level in order to move the organization toward fulfilling its mission.

Depending on the organization, three types of operational resilience requirements may be elicited: enterprise, service, and asset.

- **Enterprise**—Enterprise operational resilience requirements reflect enterprise-level needs, expectations, and constraints. These requirements affect nearly all aspects of an organization's operations. Laws and regulations are examples of this type of requirement because they broadly affect the business in which an organization operates and must be met by all organizational functions and activities. A specific example of an enterprise requirement is “all health-related information that is covered by HIPAA regulations must be kept confidential to health workers and patients.”

- **Service**—Service requirements establish the resilience needs of a service in pursuit of its mission. But because the capability of a service to meet its mission is directly related to the resilience of the assets that support the service, service requirements must reflect and be congruent with the operational resilience requirements of supporting assets. Service requirements tend to concentrate on the service’s availability and recoverability, but these quality attributes can be directly affected by failure to meet the confidentiality, integrity, and availability requirements of people, information, technology, and facilities.
- **Asset**—Asset-specific requirements are set by the owners of the asset and are intended to establish the needs for protecting and sustaining an asset with respect to its role in supporting mission assurance of a service. In practice, asset-specific resilience requirements generally reflect the security objectives of confidentiality and integrity and the continuity requirement of availability. It must be considered that assets also may have conflicting requirements, particularly when they are deployed in supporting more than one service (e.g., a network server may support more than service). This conflict must be resolved to ensure that all services that are dependent on the asset are provided the necessary level of resilience to meet their mission.

The applicability of a specific type of resilience requirement varies depending on the asset type, as shown in Table RRD-1.

Table RRD-1 Extension of Resilience Requirements to All Types of Resilience Assets

Resilience Requirement	**Asset Type**			
	People	**Information**	**Technology**	**Facilities**
Confidentiality	—	x	—	—
Integrity	\	x	x	x
Availability	x	x	x	x

There are many ways in which an organization can elicit resilience requirements. Strategic planning efforts may establish enterprise-level requirements, as would direct interviewing of vital organizational managers. Service-level requirements may be established by owners of the service (e.g., an organizational unit or a line of business). Asset-level requirements may be established through regular security risk assessment and business impact analysis activities and through directly interviewing the owners of the assets, who understand their importance to services and are responsible for their productivity and resilience.

All resilience requirements must be analyzed for conflicts and interdependencies and must be validated against and support the accomplishment of enterprise-level organizational drivers (goals, objectives, and critical success factors). Otherwise, the protection and sustainment strategies developed and implemented for assets and services will not align with what the organization needs to accomplish in order to remain viable.

The development of resilience requirements typically includes the following activities:

- identifying organizational drivers and preparing these work products so that they can be used as the foundation for setting resilience requirements
- developing and communicating enterprise-level requirements
- developing and communicating service- and asset-level requirements

- regularly analyzing the requirements to ensure alignment with current organizational drivers, to identify conflicts between enterprise- and asset-level requirements, and to satisfy operational constraints
- validating the requirements against organizational drivers and operational constraints

The Resilience Requirements Development process area has three specific goals:

1. The Identify Enterprise Requirements goal addresses the development of enterprise-level requirements that potentially affect all services and assets.
2. The Develop Service Requirements goal addresses the development of service-level requirements through the identification of asset requirements and the assignment of enterprise requirements to services.
3. The Analyze and Validate Requirements goal addresses the analysis of service-level requirements to ensure that they support strategic drivers and the resolution of conflicting requirements.

The goals of the Resilience Requirements Development process area are supported and managed long term by achievement of the goals in the Resilience Requirements Management process area.

Related Process Areas

The identification of high-value assets and the assignment of resilience requirements to assets and services are performed in the Asset Definition and Management process area.

The identification of high-value services is performed in the Enterprise Focus process area.

The identification and prioritization of risks to high-value services and supporting assets is performed in the Risk Management process area.

Resilience requirements are managed in the Resilience Requirements Management process area.

Summary of Specific Goals and Practices

Goals	**Practices**
RRD:SG1 Identify Enterprise Requirements	RRD:SG1.SP1 Establish Enterprise Resilience Requirements
RRD:SG2 Develop Service Requirements	RRD:SG2.SP1 Establish Asset Resilience Requirements
	RRD:SG2.SP2 Assign Enterprise Resilience Requirements to Services
RRD:SG3 Analyze and Validate Requirements	RRD:SG3.SP1 Establish a Definition of Required Functionality
	RRD:SG3.SP2 Analyze Resilience Requirements
	RRD:SG3.SP3 Validate Resilience Requirements

Specific Practices by Goal

RRD:SG1 Identify Enterprise Requirements

The organization's enterprise-level resilience requirements are identified and established.

Enterprise-level operational resilience requirements are derived from identified organizational needs. At a strategic level, they establish the requirements that the enterprise imposes on all functions and activities in the organization, as well as externally imposed requirements.

RRD:SG1.SP1 Establish Enterprise Resilience Requirements

The resilience requirements of the enterprise are established.

Enterprise-level resilience requirements directly reflect strategic drivers and compliance obligations. They establish the requirements that the enterprise imposes on all its functions and activities. This includes any external requirements that the enterprise inherits from its core business affiliations and competitive environment. Regulatory requirements are a common example of external requirements.

Enterprise-level requirements may also be derived from the results of enterprise risk identification activities such as security risk assessments and business impact analyses.

Sources of enterprise requirements include

- strategic objectives that must be supported and promoted by all organizational functions
- laws and regulations to which the enterprise is subject because of its geographical location or type of business, for example:
  - confidentiality and privacy regulations such as those included in HIPAA or GLBA
  - local laws that restrict disclosure or modification of information, as well as security breach notification
- business affiliations that may impose standards and restrictions for the good of all organizations in the business, for example, availability regulations that may be imposed on all organizations whose operations are tightly connected, such as financial institutions and telecommunications service providers
- organizational policies that attempt to enforce and reinforce acceptable behaviors across the enterprise, such as keeping payroll data confidential
- agreements with external entities that may impose additional constraints on the enterprise

Compliance obligations that may result in or form the basis for enterprise requirements are identified and managed in the Compliance process area.

Strategic objectives and critical success factors that may result in or form the basis for enterprise requirements are identified and managed in the Enterprise Focus process area.

Typical work products

1. Enterprise requirements list (derived from strategic objectives, laws, regulations, and policies)

Subpractices

1. Identify the legal, statutory, regulatory, and contractual requirements that an organization and all of its external entities (such as business partners, contractors, and service providers) are required to satisfy.
2. Identify business-specific constraints.
3. Identify the principles, objectives, and business requirements for processing, storing, and transmitting information that an organization has developed to support its operations.
4. Identify organizational strategic objectives, critical success factors, policies, or other indicators of importance that could result in enterprise requirements.
5. Develop and communicate a list of enterprise requirements that affect all organizational units and lines of business.

RRD:SG2 Develop Service Requirements

The resilience requirements for services are developed and established based on the service mission and the requirements of supporting assets.

The needs of the organization are satisfied by consistent and efficient performance of services. These services depend on the contributions and support of assets to meet their missions. Thus, the resilience of these assets is paramount to mission assurance.

Assets for which resilience requirements are typically developed include

- people (to control and monitor the services)
- information assets (to be used as input to and output from the processes)
- technology assets (on which the services are dependent to accomplish their missions)
- facilities (in which the other assets are located in order to execute the services to completion)

Owners of services are typically the best sources for developing service-level resilience requirements. However, these requirements are essentially derived from a consideration of the requirements of associated assets. Thus, the assets associated with a service must first be identified, then the contribution of the assets to achieving the service’s mission must be determined, and finally the specific requirements of the assets must be identified. The link between service requirements and the requirements of associated assets is explicit and iterative. Thus, this process requires service owners to work with asset owners (if they are different) to develop requirements that reflect the service’s needs at the asset level.

RRD:SG2.SP1 Establish Asset Resilience Requirements

The resilience requirements of assets as they relate to the services they support are established.

The needs of the organization and the protection and continuity requirements of services are translated into asset-level resilience requirements. In practical application, this requires three distinct activities:

- identification of high-value services (High-value services are those on which the success of the organization’s mission is dependent.)
- identification and association of assets to organizationally high-value services (Mission assurance of services relies on the consistent and effective productivity of related assets—people, technology, information, and facilities. The needs of the service in meeting its mission guide the development of asset-level resilience requirements.)
- development of asset-level requirements based on the asset’s deployment in, contributions to, and support of associated services

Because of the association between services and assets, the resilience requirements of a service are essentially represented by the collective resilience requirements of associated assets.

Typical work products

1. List of organizationally high-value services
2. Services map (that details relationships between a service, associated business processes, and associated assets)
3. List of asset-specific resilience requirements (for each asset associated with an organizationally high-value service)

Subpractices

1. Interview asset owners to determine specific asset-level requirements.
2. Perform information security risk assessment *(refer to the Risk Management process area)* and/or business impact analysis to identify risks that must be reflected in asset requirements.
3. Document confidentiality, integrity, and availability requirements for each service-related asset.

   The identification and prioritization of services that are vital for meeting the organization’s mission are performed in the Enterprise Focus process area.

   The identification of assets and the association of these assets to the services that they support are performed in the Asset Definition and Management process area.

RRD:SG2.SP2 Assign Enterprise Resilience Requirements to Services

Enterprise requirements that affect services are assigned to the services.

The collective set of resilience requirements for a service is not complete until enterprise requirements have been assigned to the service and its associated assets. In some cases, this will cause conflict because an enterprise requirement may be more stringent than a requirement that has already been set for an asset based on its association with a service. For example, an information asset may have no confidentiality requirement based on how it is used in supporting a service, but because it is health-related information, it might be subject to confidentiality and privacy regulations that impose constraints. Thus, the association of enterprise requirements to service and asset requirements may alter these requirements.

Typical work products

1. List of enterprise requirements (that are relevant to a service)
2. List of revised asset-specific resilience requirements

Subpractices

1. Identify enterprise-level requirements that are applicable to each service and associated asset.
2. Assign enterprise-level requirements to services and associated assets.

RRD:SG3 Analyze and Validate Requirements

The resilience requirements for services are analyzed and validated.

Requirements must be analyzed and validated to ensure that they are aimed at providing the level of resilience that assets need to fulfill their roles in support of a service. The requirements are analyzed by first establishing a baseline understanding of the necessary functionality of an asset and then by determining whether the requirements meet enterprise resilience requirements, standards, regulatory factors, contracts with external entities, etc. The requirements are also analyzed to determine whether there are additional organizational constraints that must be considered before requirements are established. Finally, asset-level requirements are given a careful examination to ensure that they adequately specify what is needed to protect and sustain an asset commensurate with the contribution of the asset to accomplishing a service mission. Conflicts that arise through analysis and validation are identified and addressed.

RRD:SG3.SP1 Establish a Definition of Required Functionality

A definition of the required functionality of assets in the context of the services they support is established and maintained.

The expected behaviors of assets as they are associated with services are established to provide a baseline against which asset-level resilience requirements can be analyzed and validated. This provides a foundation for establishing that the requirements are properly aligned with organizational drivers and that they will provide the appropriate level of resilience when translated into protective controls and service continuity plans.

The required functionality of an asset in the context of a service may be included as part of the asset’s description as produced in the Asset Definition and Management process area.

Typical work products

1. Asset functionality description

Subpractices

1. Document the asset functionality description for each asset that is associated with one or more services.

   Because the asset may be associated with one or more services, include in the baseline documentation all of the services with which the asset is associated and the required level of asset functionality in *each* instance.

RRD:SG3.SP2 Analyze Resilience Requirements

The requirements of assets are analyzed to identify conflicts, interdependencies, and shared requirements.

The analysis of asset resilience requirements is performed for two basic reasons: to identify conflicts between the requirements and the required functionality of the asset based on its association with a service, and to identify conflicts that arise because the asset is vital to more than one service requiring differing levels of resilience. This often occurs with information, technology, and facility assets that are shared by more than one service, such as a vendor database, a network server, or a data center facility.

The analysis process is also intended to identify requirements that cannot be met or that are incongruent with the baseline functionality of the asset.

Typical work products

1. Requirements conflicts
2. Conflict mitigation action plans
3. Revised asset-level requirements

Subpractices

1. Analyze asset requirements against baseline asset functionality and identify conflicts. Make adjustments to requirements as necessary.

   Because the asset may be associated with one or more services, be sure to identify conflicts that arise as a result. Resolve each conflict by revising requirements to fit the functionality of the asset for all instances in which it supports a service.

2. Develop conflict mitigation action plans to resolve requirements deficiencies and conflicts that result from analysis and validation activities.
3. Analyze asset requirements against enterprise requirements that have been assigned to services. Revise asset requirements to reflect enterprise requirements where necessary.

RRD:SG3.SP3 Validate Resilience Requirements

Asset-level resilience requirements are validated to ensure they adequately specify what is needed to protect and sustain an asset commensurate with its value.

Asset-level requirements are objectively validated (qualitatively) to ensure that they support the required functionality of assets and their associated services. Any risks to protecting and sustaining assets that are introduced by requirements are identified and addressed. A review of the alignment between requirements and the organization's strategic drivers is performed and any missing or inadequate requirements are identified, reassessed, updated, and analyzed.

Typical work products

1. Requirements gaps
2. Revised asset requirements

Subpractices

1. Perform affinity analysis between strategic drivers (such as critical success factors) and asset requirements.
2. Carefully analyze requirements to ensure that they adequately specify what is needed to protect and sustain an asset relative to its association with a service.
3. Identify requirements gaps.
4. Revise requirements as necessary.

Elaborated Generic Practices by Goal

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

RRD:GG1 Achieve Specific Goals

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

RRD:GG1.GP1 Perform Specific Practices

Perform the specific practices of the Resilience Requirements Development process area to develop work products and provide services to achieve the specific goals of the process area.

Elaboration:

Specific practices RRD:SG1.SP1 through RRD:SG3.SP3 are performed to achieve the goals of the resilience requirements development process.

RRD:GG2 Institutionalize a Managed Process

Resilience requirements development is institutionalized as a managed process.

RRD:GG2.GP1 Establish Process Governance

Establish and maintain governance over the planning and performance of the resilience requirements development process.

Refer to the Enterprise Focus process area for more information about providing sponsorship and oversight to the resilience requirements development process.

Subpractices

1. Establish governance over process activities.

   Elaboration:

   Governance over the resilience requirements development process may be exhibited by

   - developing and publicizing higher level managers' objectives for the development of asset resilience requirements
   - sponsoring and providing oversight of policy, procedures, standards, and guidelines for effective and sufficient resilience requirements development
   - making higher level managers aware of applicable compliance obligations related to developing resilience requirements, and regularly reporting on the organization's satisfaction of these obligations to higher level managers
   - sponsoring and funding the development and regular validation of resilience requirements
   - providing guidance and assigning priorities to assets (relative to strategic objectives) that must satisfy resilience requirements
   - sponsoring regular audits and reviews to validate requirements
   - sponsoring regular audits and reviews to ensure requirements form the basis for activities to protect and sustain assets
   - identifying gaps in requirements and sponsoring actions to close the gaps
   - verifying that the process supports strategic resilience objectives and is focused on the assets and services that are of the highest relative value in meeting strategic objectives
   - reporting regularly from organizational units to higher level managers on process activities and results
   - creating dedicated higher level management feedback loops on decisions regarding the development of resilience requirements and recommendations for improving the process
   - conducting regular internal and external audits and related reporting to appropriate committees on the effectiveness of the process
   - creating formal programs to measure the effectiveness of process activities, and reporting these measurements to higher level managers

2. Develop and publish organizational policy for the process.

Elaboration:

The resilience requirements development policy should address

- responsibility, authority, and ownership for developing requirements (particularly for assets) and for all process activities
- responsibility and authority for determining the adequacy and completeness of requirements
- procedures, standards, and guidelines for
  - documenting requirements and relevant information
  - distributing requirements to relevant custodians (those who must implement the requirements relative to assets in their care or possession)
- validating requirements relative to strategies for protecting and sustaining assets commensurate with the value of the assets and the services with which they are associated
- methods for measuring adherence to policy, exceptions granted, and policy violations

RRD:GG2.GP2 Plan the Process

Establish and maintain the plan for performing the resilience requirements development process.

Elaboration:

The plan for the process of resilience requirements development should enable large-scale (either at the enterprise or organizational unit level) development of resilience requirements by owners of organizational assets (particularly information, technology, and facilities assets). The plan should also allow for the distribution of these requirements to custodians who are responsible for implementing strategies to meet the requirements for protecting and sustaining assets in their care or possession. The plan must support both internal staff involved in the process (typically asset owners) as well as external entities (which may include custodians).

Subpractices

1. Define and document the plan for performing the process.

   Elaboration:

   The services to which assets are associated have to be considered to provide insight into the level and extent of resilience requirements necessary. Thus, the plan should take into consideration the plan for establishing and prioritizing organizational services and associating them with assets.

   Refer to the Enterprise Focus process area for information about identifying organizational services and associating them with organizational assets.

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

RRD:GG2.GP3 Provide Resources

Provide adequate resources for performing the resilience requirements development process, developing the work products, and providing the services of the process.

Subpractices

1. Staff the process.

   Elaboration:

   The diversity of asset types (people, information, technology, and facilities) requires that staff assigned to the resilience requirements development process have appropriate knowledge of all assets that need to fulfill resilience requirements and the services with which they are associated.

   These are examples of staff required to perform the resilience requirements development process:

   - staff responsible for identifying enterprise operational resilience requirements such as laws, regulations, and other compliance obligations
   - service owners to identify service resilience needs such as availability and recoverability
   - asset owners and custodians to identify needs for protecting and sustaining assets
   - business continuity and disaster recovery staff
   - IT operations and service delivery staff
   - physical security staff
   - staff skilled in eliciting requirements across domains, functions, assets, and services
   - staff responsible for identifying the relationships between a service, associated business processes, and associated assets
   - staff responsible for resolving requirements conflicts
   - staff responsible for managing the process plan and for ensuring that the plan is aligned with stakeholder requirements and needs
   - external entities responsible for protecting and sustaining assets
   - staff responsible for managing external entities that have contractual obligations for meeting resilience requirements
   - internal and external auditors responsible for reporting to appropriate committees on process effectiveness

   Refer to the Organizational Training and Awareness process area for information about training staff for resilience roles and responsibilities.

   Refer to the Human Resource Management process area for information about acquiring staff to fulfill roles and responsibilities.

2. Fund the process.

   Refer to the Financial Resource Management process area for information about budgeting for, funding, and accounting for resilience requirements development.

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

Elaboration:

These are examples of tools, techniques, and methods to support the resilience requirements development process:

- tools for scenario planning and analysis
- tools, techniques, and methods for
  - eliciting, documenting, and analyzing requirements
  - validating requirements, including affinity analysis
  - performing security risk assessments and business impact analysis
- tools for requirements tracking
- methods for requirements conflict mitigation and resolution

RRD:GG2.GP4 Assign Responsibility

Assign responsibility and authority for performing the resilience requirements development process, developing the work products, and providing the services of the process.

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

Subpractices

1. Assign responsibility and authority for performing the process.

   Elaboration:

   The primary staff involved in the resilience requirements development process are service owners and asset owners and custodians.

   Refer to the Enterprise Focus process area for information about identifying organizational services and associating them with organizational assets.

   Refer to the Asset Definition and Management process area for more information about establishing asset ownership and custodianship.

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

   Elaboration:

   Responsibility and authority for performing resilience requirements development tasks can be formalized by

   - defining roles and responsibilities in the process plan
   - including process tasks and responsibility for these tasks in specific job descriptions
   - developing policy that requires organizational unit managers, line of business managers, project managers, and asset and service owners and custodians to participate in and derive benefit from the process for assets and services under their ownership
   - including process activities in staff performance management goals and objectives with requisite measurement of progress against these goals

- including process activities in contracts and service level agreements with external entities
- including process tasks in measuring the performance of external entities against contracts and service level agreements

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

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

RRD:GG2.GP5 Train People

Train the people performing or supporting the resilience requirements development process as needed.

Elaboration:

Expertise in developing resilience requirements requires a strong understanding of each type of resilience requirement (confidentiality, integrity, and availability) as well as the ability to understand strategies (including the internal control system) for protecting and sustaining the various types of assets. Knowledge across multiple functional domains of physical and logical security, business continuity, logistics, and crisis response may also be required.

Refer to the Organizational Training and Awareness process area for more information about training the people performing or supporting the process.

Refer to the Human Resource Management process area for more information about inventorying skill sets, establishing a skill set baseline, identifying required skill sets, and measuring and addressing skill deficiencies.

Subpractices

1. Identify process skill needs.

Elaboration:

Resilience requirements must be developed through working knowledge of how an asset is deployed and how it contributes to ensuring the mission of organizational services. Asset owners must be skilled in analyzing the dependencies among assets, services, and organizational goals and mission and translating these dependencies into resilience requirements that ensure that the asset is protected from threats and sustained if threatened. Functional working knowledge of the types of resilience requirements and their impact on assets is essential.

These are examples of skills required in the resilience requirements development process:

- eliciting and developing enterprise resilience requirements
- eliciting and developing service resilience requirements
- eliciting and developing asset resilience requirements
- documenting resilience requirements, including mapping them to their sources
- identifying the relationships between a service, associated business processes, and associated assets

- understanding tools, techniques, and methods that can be used to develop, analyze, and validate requirements
- establishing, implementing, and maintaining the internal control system for assets
- protecting and sustaining assets to meet their resilience requirements

2. Identify process skill gaps based on available resources and their current skill levels.
3. Identify training opportunities to address skill gaps.

Elaboration:

Information security risk assessment training can provide fundamental knowledge about resilience requirements such as confidentiality and integrity. An active knowledge of business impact analysis techniques can provide foundational knowledge about availability requirements.

Training may also be needed for staff to use requirements development tools, techniques, and methods (particularly those supported by software) to document and analyze requirements.

These are examples of training topics:

- resilience requirements (confidentiality, integrity, and availability and which types of requirements are applicable to each type of asset)
- requirements elicitation and facilitation
- requirements specification and documentation
- requirements analysis and validation
- requirements tracking
- requirements gap analysis
- requirements conflict mitigation and resolution
- establishing, implementing, and maintaining internal controls for protecting and sustaining assets
- supporting asset owners and custodians in understanding the process and their roles and responsibilities with respect to its activities
- working with external entities that have responsibility for process activities
- using process methods, tools, and techniques, including those identified in RRD:GG2:GP3 subpractice 3

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

RRD:GG2.GP6 Control Work Products

Place designated work products of the resilience requirements development process under appropriate levels of control.

Elaboration:

Changes in strategic objectives or assets (and the services with which they are associated) will necessitate changes in resilience requirements. Because resilience requirements are the basis for strategies to protect and sustain assets, changes to these requirements may in turn translate to changes in strategies, such as the type and extent of controls and changes to service continuity plans.

Changes to resilience requirements are managed in the Resilience Requirements Management process area.

These are examples of resilience requirements development work products placed under control:

- resilience requirements (enterprise, service, asset)
- services map (relationships between a service, associated business processes, and associated assets)
- asset functionality descriptions
- requirements gaps
- requirements conflicts and mitigation action plans
- process plan
- policies and procedures
- contracts with external entities

RRD:GG2.GP7 Identify and Involve Relevant Stakeholders

Identify and involve the relevant stakeholders of the resilience requirements development process as planned.

Subpractices

1. Identify process stakeholders and their appropriate involvement.

   Elaboration:

   These are examples of stakeholders of the resilience requirements development process:

   - owners and custodians of assets, including
     - human resources (for people assets)
     - information technology staff (for technology assets)
     - staff responsible for physical security (for facility assets)
   - service and business process owners
   - organizational unit and line of business managers responsible for assets and their associated services
   - staff involved in business impact analysis and security risk assessment
   - staff responsible for identifying and managing operational risks to assets and services
   - staff responsible for establishing, implementing, and maintaining an internal control system for assets
   - external entities that are involved in ensuring that assets under their control meet their resilience requirements
   - internal and external auditors

   Stakeholders are involved in various tasks in the resilience requirements development process, such as

   - planning for the development of resilience requirements
   - participating in the elicitation and identification of enterprise, service, and asset resilience requirements

- resolving issues with the understanding of the requirements
- resolving requirements gaps and conflicts
- communicating requirements to those with a need to know
- identifying requirements conflicts
- managing operational risks to assets
- managing relationships with external entities that support process activities
- reviewing and appraising the effectiveness of process activities
- resolving issues in the resilience process

2. Communicate the list of stakeholders to planners and those responsible for process performance.
3. Involve relevant stakeholders in the process as planned.

RRD:GG2.GP8 Measure and Control the Process

Measure and control the resilience requirements development process against the plan for performing the process and take appropriate corrective action.

Refer to the Monitoring process area for more information about the collection, organization, and distribution of data that may be useful for measuring and controlling processes.

Refer to the Measurement and Analysis process area for more information about establishing process metrics and measurement.

Refer to the Enterprise Focus process area for more information about providing process information to managers, identifying issues, and determining appropriate corrective actions.

Subpractices

1. Measure actual performance against the plan for performing the process.
2. Review accomplishments and results of the process against the plan for performing the process.

Elaboration:

These are examples of metrics for the resilience requirements development process:

- percentage of enterprise requirements that have been communicated to all organizational units and lines of business
- percentage of services with incomplete or no stated requirements
- percentage of assets with incomplete or no stated requirements
- percentage of service owners participating in the development of requirements
- percentage of asset owners participating in the development of requirements
- percentage of documented requirements that have not been implemented
- percentage of assets for which the required level of functionality of the asset is not documented for all services it supports
- percentage of assets with requirements revisions die to:
- conflicts resulting from associations with multiple services

  - requirements deficiencies
  - enterprise requirements
  - requirements gaps
- percentage of requirements whose adequacy has not been validated percentage of asset requirements conflicts for which mitigation plans have been developed but not implemented
- percentage of requirements that have not been analyzed to identify conflicts and interdependencies
- percentage of requirements whose adequacy has not been validated
- elapsed time between identification of new assets and the development of requirements for these assets (mean, median)
- costs of developing, analyzing, validating, documenting, and tracking requirements
- percentage of service continuity test failures caused by incorrect or missing requirements
- percentage of incidents caused by incorrect or missing requirements

3. Review activities, status, and results of the process with the immediate level of managers responsible for the process and identify issues.

Elaboration:

The results of periodic reviews should be elevated to higher level managers to ensure that strategies for protecting and sustaining assets are in alignment with the resilience requirements of these assets (i.e., able to satisfy the requirements) as well as with the organization’s enterprise resilience requirements and strategic objectives.

Periodic reviews of the resilience requirements development process are needed to ensure that

- all high-value services and assets have defined resilience requirements, including newly acquired assets
- the service-business process-asset mapping is accurate and current
- asset owners are involved in the process of developing and validating requirements
- requirements are being communicated to custodians through formal channels
- status reports are provided to appropriate stakeholders in a timely manner
- requirements issues are referred to the risk management process when necessary
- actions requiring management involvement are elevated in a timely manner
- the performance of process activities is being monitored and regularly reported
- key measures are within acceptable ranges as demonstrated in governance dashboards or scorecards and financial reports
- actions resulting from internal and external audits are being closed in a timely manner

4. Identify and evaluate the effects of significant deviations from the plan for performing the process.

5. Identify problems in the plan for performing and executing the process.

6. Take corrective action when requirements and objectives are not being satisfied, when issues are identified, or when progress differs significantly from the plan for performing the process.

7. Track corrective action to closure.

RRD:GG2.GP9 Objectively Evaluate Adherence

Objectively evaluate adherence of the resilience requirements development process against its process description, standards, and procedures, and address non-compliance.

Elaboration:

Objective evaluation of the resilience requirements development process is intended to ensure that high-quality resilience requirements are being developed, analyzed, and validated for assets. Because these requirements form the basis for an "engineering" approach to operational resilience management, the process is foundational to all other engineering activities in the model. Inconsistent adherence to the process can result in a lack of requirements or poorly developed requirements, which can cause cascading effects on managing operational resilience that will be realized in other process areas.

These are examples of activities to be reviewed:

- establishing enterprise, asset, and service resilience requirements
- obtaining commitments to requirements by owners and custodians
- analyzing requirements and resolving conflicts
- identifying and resolving requirements gaps
- aligning stakeholder requirements with the process plan
- assigning responsibility, accountability, and authority for process activities
- determining the adequacy of process reports and reviews in informing decision makers regarding the performance of operational resilience management activities and the need to take corrective action, if any

These are examples of work products to be reviewed:

- business impact analysis and security risk assessment results
- enterprise, service, and asset resilience requirements
- services map
- commitment documents
- requirements baseline and database
- requirements traceability matrix
- corrective actions, including conflict mitigation plans
- process plan and policies
- issues that have been referred to the risk management process
- process methods, techniques, and tools
- metrics for the process *(Refer to RRD:GG2.GP8 subpractice 2.)*
- contracts with external entities

RRD:GG2.GP10 Review Status with Higher Level Managers

Review the activities, status, and results of the resilience requirements development process with higher level managers and resolve issues.

Elaboration:

Assets that do not have resilience requirements or have poorly developed requirements should be brought to the attention of higher level managers as a symptom of potential process inadequacies. Audits of the process should be conducted regularly for a wide range of organizational assets to ensure that the process is functioning properly across organizational units and the enterprise.

Refer to the Enterprise Focus process area for more information about providing sponsorship and oversight to the operational resilience management system.

RRD:GG3 Institutionalize a Defined Process

Resilience requirements development is institutionalized as a defined process.

RRD:GG3.GP1 Establish a Defined Process

Establish and maintain the description of a defined resilience requirements development process.

Elaboration:

The definition, analysis, and validation of asset resilience requirements are best performed at a level commensurate with direct ownership of the asset. Thus, this process may often be carried out at the organizational unit level. However, to ensure consistency of requirements across organizational units, the process must be tailored from the organization's enterprise process definition.

Establishing and tailoring process assets, including standard processes, are addressed in the Organizational Process Definition process area.

Establishing process needs and objectives and selecting, improving, and deploying process assets, including standard processes, are addressed in the Organizational Process Focus process area.

Subpractices

1. Select from the organization's set of standard processes those processes that cover the resilience requirements development process and best meet the needs of the organizational unit or line of business.
2. Establish the defined process by tailoring the selected processes according to the organization's tailoring guidelines.
3. Ensure that the organization's process objectives are appropriately addressed in the defined process, and ensure that process governance extends to the tailored processes.
4. Document the defined process and the records of the tailoring.

5. Revise the description of the defined process as necessary.

RRD:GG3.GP2 Collect Improvement Information

Collect resilience requirements development work products, measures, measurement results, and improvement information derived from planning and performing the process to support future use and improvement of the organization's processes and process assets.

Elaboration:

These are examples of improvement work products and information:

- information about the types and extent of requirements changes (from baseline) *(Refer to the Resilience Requirements Management process area for information about the handling of requirements changes.)*
- requirements coverage (of all identified assets and services)
- requirements conflicts
- gaps in requirements
- the ease of understanding and traceability of requirements
- the level of asset owner and custodian commitment to the requirements
- metrics and measurements of the viability of the process *(Refer to RRD:GG2.GP8 subpractice 2.)*
- changes and trends in operating conditions, risk conditions, and the risk environment that affect resilience requirements and the process
- lessons learned in post-event review of asset incidents and disruptions in continuity (including confidentiality, integrity, availability, and privacy)
- conflicts and risks arising from dependencies on external entities
- resilience requirements that are not being satisfied or are being exceeded

Establishing the measurement repository and process asset library is addressed in the Organizational Process Definition process area. Updating the measurement repository and process asset library as part of process improvement and deployment is addressed in the Organizational Process Focus process area.

Subpractices

1. Store process and work product measures in the organization's measurement repository.
2. Submit documentation for inclusion in the organization's process asset library.
3. Document lessons learned from the process for inclusion in the organization's process asset library.
4. Propose improvements to the organizational process assets.