Software Engineering Institute

CERT® Resilience Management Model, Version 1.2

Resilience Requirements Management (RRM)

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/

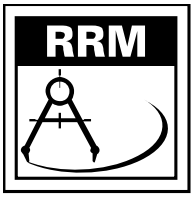
Carnegie Mellon

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

DM-0003234

RESILIENCE REQUIREMENTS MANAGEMENT

Engineering



Purpose

The purpose of Resilience Requirements Management is to manage the resilience requirements of high-value services and associated assets and to identify inconsistencies between these requirements and the activities that the organization performs to meet the requirements.

Introductory Notes

In conjunction with the Resilience Requirements Development process area, the Resilience Requirements Management process area seeks to define the life cycle of resilience requirements—from inception, development, or acquisition to application, monitoring and measurement, and change management. In reality, resilience requirements constantly evolve as the organization encounters changes in strategic direction, operational complexity, and new or evolving risk environments. Unfortunately, requirements often are not revisited to ensure alignment with strategies for protecting and sustaining services and assets, potentially affecting the resilience of these services and ultimately the organization's mission. Thus, the organization must implement and make a commitment to dedicated processes that aim to constantly monitor and adjust requirements as these triggers for change are encountered.

The Resilience Requirements Management process area aims to ensure that the requirements that are established in the Resilience Requirements Development process area (or are otherwise acquired) remain viable for each high-value asset associated with a high-value service until it is retired (either because the asset is retired or its relative value is reduced) or until it is changed due to one or more organizational triggers. In addition, Resilience Requirements Management defines the organization's responsibility for monitoring the effectiveness of requirements (for protecting service-related assets and ensuring their continuity) and for recognizing when changes to requirements are necessary. Finally, the evolution of requirements often necessitates that an organization revisit the goals and practices in the Resilience Requirements Development process area because organizational drivers must be reestablished, new or revised enterprise-level or asset-level requirements must be developed, or changes to requirements must be analyzed and revalidated. The iterative nature of the Resilience Requirements Development and Resilience Requirements Management process areas is necessary to ensure that asset-level resilience requirements satisfactorily reflect and support strategic drivers, and this in turn supports the level of operational resilience that the organization desires.

The Resilience Requirements Management process area has one specific goal—to manage resilience requirements. In practice, this requires that the organization obtain and promote an understanding of the requirements, ensure commitment to satisfying the requirements, manage changes to the requirements, establish traceability of the requirements, and identify inconsistencies between the requirements and the activities that the organization performs to satisfy them.

Related Process Areas

The identification, development, documentation, and analysis of resilience requirements are performed in the Resilience Requirements Development process area.

The responsibility for managing requirements at the asset level is established in the Asset Definition and Management process area.

Ensuring that requirements reflect the protection and continuity needs of the owners of the assets is performed in the Resilience Requirements Development process area.

Identifying and establishing the ownership of the assets and the corresponding responsibilities for establishing and validating resilience requirements are performed in the Asset Definition and Management process area.

The monitoring and control of the satisfaction of resilience requirements for high-value business processes, services, and associated assets are performed in the Monitoring process area.

Summary of Specific Goals and Practices

Goals	Practices
RRM:SG1 Manage Requirements	RRM:SG1.SP1 Obtain an Understanding of Resilience Requirements
	RRM:SG1.SP2 Obtain Commitment to Resilience Requirements
	RRM:SG1.SP3 Manage Resilience Requirements Changes
	RRM:SG1.SP4 Maintain Traceability of Resilience Requirements
	RRM:SG1.SP5 Identify Inconsistencies Between Resilience Requirements and Activities Performed to Meet the Requirements

Specific Practices by Goal

RRM:SG1 Manage Requirements

Resilience requirements are actively managed and inconsistencies between requirements and the activities necessary to satisfy them are identified.

The requirements defined and established in Resilience Requirements Development are managed over the life of the associated assets by

- identifying and managing changes to requirements (by establishing change triggers and criteria)
- establishing a shared view and understanding of requirements between owners and custodians
- maintaining the relationship between requirements and associated assets and services
- identifying inconsistencies between requirements and associated assets and services, and the activities performed to satisfy the requirements
- taking corrective action when requirements are not being satisfied

RRM:SG1.SP1 Obtain an Understanding of Resilience Requirements

An understanding of resilience requirements is obtained from providers to ensure consistency and accuracy.

The identification and implementation of asset resilience requirements require cooperation between service owners, asset owners, and asset custodians. This cooperation must be based on a mutual and shared understanding of requirements.

Resilience requirements can come from many different sources, but asset owners have the ultimate responsibility for identifying, collecting, and establishing these requirements and for communicating these requirements to all those with a need to know (e.g., owners of an information asset such as medical records would be responsible for setting the confidentiality, integrity, and availability requirements for these records relative to the services they support). The requirements that asset owners develop are based on their implicit understanding of the relative value of the assets (as defined by the services to which they are associated) as well as the needs of the organization (as established in work products such as strategic drivers). They are also influenced by enterprise-level requirements and the results of risk assessments and business impact analyses.

Establishing ownership of the assets and the corresponding responsibilities for establishing and validating resilience requirements is performed in the Asset Definition and Management process area.

Asset custodians must ensure that they clearly and completely understand the requirements so that there is a shared vision of the need for protecting and sustaining assets. Custodians must ensure that they act only on the requirements from authorized providers (generally asset owners or their approved designees). Custodians must agree to the requirements and must identify any organizational constraints they may know of in satisfying the requirements so that the constraints can be communicated to owners for their consideration and approval. The agreement between owners and custodians on how assets are to be protected and sustained is crucial in managing operational resilience.

Typical work products

1. Criteria for evaluation and acceptance of requirements (by custodians)
2. Agreed-to set of asset requirements (between asset owners and asset custodians)

Subpractices

1. Establish objective criteria for the evaluation and acceptance of requirements.
2. Analyze requirements to ensure that the established evaluation and acceptance criteria are met.
3. Reach an understanding (between owners and custodians) on the requirements so that custodians can commit to them.

RRM:SG1.SP2 Obtain Commitment to Resilience Requirements

Commitments to resilience requirements are obtained from those who are responsible for satisfying the requirements.

The resilience requirements set by asset owners require two actions to ensure implementation: (1) they must be communicated to all custodians who need to know them, and (2) custodians must make a commitment to implement and manage the requirements. Because requirements represent a wide range of needs for protecting assets, custodians in turn may represent a wide range of organizational entities and activities, so this practice may be extensive.

Owners must commit to developing and monitoring the requirements, and custodians must commit to performing activities that are commensurate with protecting and sustaining assets. Owners must ensure that commitments have been obtained from custodians both internal and external to the organization to implement the requirements as provided and to manage to the requirements as they change and evolve.

Typical work products

1. Documented commitments to requirements and requirement changes (e.g., service level agreements)

Subpractices

1. Document and communicate requirements through service level agreements between asset owners and custodians.
2. Document the custodian's understanding of requirements and obtain sign-off.

RRM:SG1.SP3 Manage Resilience Requirements Changes

Changes to resilience requirements are managed as conditions dictate.

The conditions under which organizations operate are continually changing. As a result, the risk environment for services and associated assets continues to evolve as well. An organization must become very adept at recognizing changes in conditions that precipitate considerations for changes in asset resilience requirements.

Managing changes to requirements involves consideration of several distinct activities:

- identifying change triggers and criteria

  These are examples of triggers that might require changes in resilience requirements:
  - changes in the organization's mission, goals, objectives, or critical success factors
  - changes in organizational lines of business or geographical operations
  - changes in organizational structure, including staff changes
  - changes that result in outsourcing services and assets or in changing current external entity relationships
  - market and economic conditions

- social or political conditions, or geographically induced constraints
- identification of internal or external fraud or the realization of risk and impact to the organization
- redeployment or association of assets to new or different services
- identification of conditions that would result in exposure to new risks (via risk assessment processes)

- identifying associated assets that may be affected by these triggers
- assessing the impact of changes on asset requirements
- identifying and documenting changes to existing requirements (or identifying new requirements, if necessary)
- communicating changes to requirements to those who are responsible for their implementation (custodians)

Change management for resilience requirements is a continuous process and therefore requires that the organization effectively assign responsibility and accountability for it. The organization must independently monitor that the change management process is operational and that asset-level resilience requirements have been updated on a regular basis so that they remain in direct alignment with organizational drivers. In most cases, these responsibilities will fall to asset owners as part of their management of the assets over their life cycles.

Typical work products

1. Requirements baseline
2. Requirements status
3. Requirements database, including change history
4. Requirements change criteria
5. Requirements change requests

Subpractices

1. Establish a requirements baseline from which changes will be managed.
2. Develop and document criteria for establishing when a change in requirements must be considered.

   Ensure that these criteria are commensurate with the organization's risk tolerances.
3. Analyze results of security risk assessments and/or business impact analysis to identify changes to requirements that are related to risk response.
4. Document the requirements changes.
5. Maintain a requirements change history with rationale for performing the changes.
6. Evaluate the impact of requirements changes on existing activities and commitments for protecting and sustaining assets and services.

7. Establish communications channels to ensure custodians are aware of changes in requirements.

   Update service level agreements with custodians if necessary to reflect commitment to changes.

RRM:SG1.SP4 Maintain Traceability of Resilience Requirements

Traceability between resilience requirements and the activities performed to satisfy the requirements is established.

The development, implementation, and monitoring of resilience requirements necessitate that they be traceable from originating source to assets, and vice versa. Often, there is not a simple one-to-one relationship between requirement and asset because, in practical application, requirements are usually translated and decomposed into lower level and discipline-specific (i.e., security and business continuity) activities. This is further complicated by two additional realities:

- A single resilience requirement may be associated with one asset or, more realistically, more than one asset. For example, a service that must be available 24 hours per day, 7 days per week will generate availability requirements for associated people, supporting application systems and technology components, information and data, and the facilities in which these assets are accessible and productive.
- Assets may have more than one set of resilience requirements coming from different organizational constraints and owners and the enterprise, often in direct conflict.

This specific practice ensures that the source of the requirements can be traced to all of the assets that are the subject of the requirements, which is particularly important when requirements or assets undergo changes. In addition, this specific practice requires that the organization be able to trace requirements from assets back to their sources so that responsibility and accountability for the requirements can be ascertained and that changes can be more effectively accomplished and conflicts effectively resolved.

Resolving requirements conflicts is addressed in the Resilience Requirements Development process area.

Typical work products

1. Requirements traceability matrix
2. Requirements tracking system

Subpractices

1. Document requirements and their source or origination as part of an asset profile or documentation.

   Revise the profile as requirements change to ensure it reflects current asset needs.

   The maintenance of asset profiles is addressed in the Asset Definition and Management process area.

2. Maintain requirements traceability.

Ensure traceability is maintained from strategies to protect and sustain services and assets to resilience requirements intended to implement these strategies to activities performed to satisfy the requirements.

3. Generate a requirements traceability matrix.

RRM:SG1.SP5 Identify Inconsistencies Between Resilience Requirements and Activities Performed to Meet the Requirements

Inconsistencies between resilience requirements and the activities performed to satisfy the requirements are identified and managed.

The monitoring and control of the satisfaction of resilience requirements for high-value services and associated assets are performed in the Monitoring process area.

Custodians make commitments to perform activities and implement controls that are consistent with resilience requirements and that ensure the satisfaction of those requirements. This specific practice aims to ensure that custodians are capable and prepared to meet the requirements to which they have made commitments (whether or not they are under the direct control of the organization).

Because assets may derive requirements from more than one source, it is possible that custodians in good faith commit to the requirements but in reality are constrained in satisfying them. Identifying these inconsistencies proactively can help the organization to resolve conflicts, to reroute work as necessary, or to negotiate with owners to make changes to requirements as needed.

Typical work products

1. Documentation of inconsistencies
2. Corrective actions

Subpractices

1. Review the planned or implemented activities for consistency with requirements. Identify any changes made to the requirements.
2. Document custodial constraints that may impede satisfaction of requirements and update requirements as necessary *(refer to RRM:SG1.SP3)*.
3. Identify changes that have to be made in activities (or planned activities) to ensure satisfaction of requirements as specified.
4. Initiate corrective actions to enforce alignment between requirements and activities.

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 Management process area.

RRM:GG1 Achieve Specific Goals

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

RRM:GG1.GP1 Perform Specific Practices

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

Elaboration:

Specific practices RRM:SG1.SP1 through RRM:SG1.SP5 are performed to achieve the goals of the resilience requirements management process.

RRM:GG2 Institutionalize a Managed Process

Resilience requirements management is institutionalized as a managed process.

RRM:GG2.GP1 Establish Process Governance

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

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

Subpractices

1. Establish governance over process activities.

   Elaboration:

   Governance over the resilience requirements management process may be exhibited by

   - developing and publicizing higher level managers' objectives for managing asset resilience requirements
   - sponsoring and providing oversight of policy, procedures, standards, and guidelines for effective management of resilience requirements, including traceability and change control
   - sponsoring regular audits and reviews to ensure alignment between requirements and resilience activities
   - making higher level managers aware of applicable compliance obligations related to managing resilience requirements, and regularly reporting on the organization's satisfaction of these obligations to higher level managers
   - sponsoring and funding the management of resilience requirements, including change control
   - 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 management 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 management policy should address

- responsibility, authority, and ownership for managing requirements (particularly for assets) and for all process activities
- responsibility and authority for identifying requirements inconsistencies and performing corrective actions
- procedures, standards, and guidelines for
  - documenting acquired requirements and relevant information
  - distributing requirements and requirements changes to the custodians who must implement the requirements relative to assets in their care or possession
  - documenting commitments in the form of service level agreements
  - regular updating of requirements, reconciliation, and change control
  - requirements tracking and traceability
- methods for measuring adherence to policy, exceptions granted, and policy violations

RRM:GG2.GP2 Plan the Process

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

Elaboration:

The plan for the process of resilience requirements management should enable large-scale (at the enterprise or organizational unit level, whichever is appropriate) management 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) and external entities (which may include custodians). The plan must support managing requirements that are developed as part of the resilience requirements development process, as well as requirements acquired from other internal and external sources.

Subpractices

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

Elaboration:

Special consideration may be given to the means of collecting and organizing requirements from all identified sources so that they can be managed by this process.

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

RRM:GG2.GP3 Provide Resources

Provide adequate resources for performing the resilience requirements management 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 management 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 management process:

   - asset owners and custodians
   - business continuity and disaster recovery staff
   - IT operations and service delivery staff
   - physical security staff
   - staff skilled in understanding requirements across domains, functions, assets, and services
   - staff responsible for
     - reconciling requirements conflicts and inconsistencies
     - requirements change control
     - requirements tracking and traceability
     - the process plan, ensuring it is aligned with stakeholder requirements and needs
     - managing external entities that have contractual obligations for meeting resilience requirements
   - external entities responsible for protecting and sustaining assets
   - 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 management.

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 management process:

   - tools, techniques, and methods for
     - requirements elicitation
     - requirements documentation
     - requirements analysis
     - requirements change control
   - requirements database, including change history
   - requirements tracking system
   - tools for requirements traceability
   - methods for resolving inconsistencies between requirements and activities performed to meet requirements

RRM:GG2.GP4 Assign Responsibility

Assign responsibility and authority for performing the resilience requirements management 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 management 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 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 management 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 requiring organizational unit managers, line of business managers, project managers, and asset and services owners and custodians to participate in and derive benefit from the process for assets and services under their ownership or custodianship
- 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.

RRM:GG2.GP5 Train People

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

Elaboration:

Expertise in managing 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:

   Effective management of resilience requirements (including changes to requirements) must be informed by working knowledge of how an asset is deployed and how it contributes to assuring the mission of organizational services. Asset owners and custodians must be skilled in preserving the dependencies among assets, services, and organizational mission and goals that have been translated into resilience requirements. 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 management process:

   - ability to understand and define the desired outcomes of resilience requirements

- negotiation skills
- project management skills, including estimating time, costs, and resources to manage resilience requirements and changes to requirements
- ability to use tools, techniques, and methods for managing resilience requirements, including tracking, traceability, and change control
- requirements change management skills (at the enterprise, service, and asset levels)
- ability to maintain the relationships between a service, associated business processes, and associated assets
- ability to maintain the internal control system for assets
- ability to protect and sustain 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 management tools, techniques, and methods, particularly for requirements tracking and change control, which may be performed through the use of specialized application systems and databases.

   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 management tools, including requirements tracking
   - configuration and change management practices
   - negotiation and conflict resolution
   - 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 RRM:GG2:GP3 subpractice 3

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

RRM:GG2.GP6 Control Work Products

Place designated work products of the resilience requirements management 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 and services, changes to these requirements may in turn translate to changes in strategies, including the type and extent of controls, changes to service continuity plans, etc.

RRM:SG1.SP3 specifically addresses the change control process over resilience requirements. RRM:GG2.GP6 generically covers all work products of the resilience requirements management process.

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

- resilience requirements
- requirements baseline
- requirements status
- requirements database
- requirements traceability matrix
- requirements tracking system
- service level agreements
- documentation of inconsistencies and corrective actions
- process plan
- policies and procedures
- contracts with external entities

RRM:GG2.GP7 Identify and Involve Relevant Stakeholders

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

Subpractices

1. Identify process stakeholders and their appropriate involvement.

   Elaboration:

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

   - owners and custodians of assets, including
     - human resources staff (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 management process, such as

- planning for the management of resilience requirements
- resolving issues with the understanding of the requirements
- assessing the impact of requirements changes
- communicating requirements changes to those with a need to know
- identifying inconsistencies between requirements and the activities performed to meet the requirements
- 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 process

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

RRM:GG2.GP8 Measure and Control the Process

Measure and control the resilience requirements management 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 management process:

- percentage of assets for which agreement between asset owners and custodians on asset requirements has not been reached
- percentage of service level agreements between asset owners and custodians that are pending signoff due to requirements issues
- percentage of asset custodians who accept responsibility for implementing requirements, if applicable
- percentage of documented, agreed-to requirements that have not been implemented as scheduled
- percentage of asset owners participating in managing changes to requirements for the assets they own
- number of approved requirements changes by asset category or type, by asset, by service, and by change trigger and criteria
- number of unapproved requirements changes
- number of approved requirements changes that have not been communicated to asset custodians (via defined channels or SLAs)
- percentage of requirements change requests whose disposition is pending beyond schedule
- percentage of approved requirements changes whose implementation is pending beyond schedule
- percentage of requirements changes that are not subject to the organization's change control process
- costs of analyzing, managing, documenting, and tracking changes to requirements
- percentage of requirements that are not traced to a source or origination (documented in the asset profile)
- percentage of resilience activities that are not traced to a requirement
- number of inconsistencies detected between requirements and the activities in place to satisfy the requirements
- number of corrective actions to align requirements and the activities required to satisfy them that are open beyond threshold (as scheduled)
- elapsed time between major updates to assets (such as being associated with a new service) and updates to the requirements for these assets (mean, median)

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

Elaboration:

The results of periodic reviews should be elevated to higher level managers to ensure that the strategies for protecting and sustaining assets continue to be in alignment with (1) their resilience requirements (that is, able to satisfy the requirements) as requirements change and (2) the organization's enterprise resilience requirements and strategic objectives.

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

- requirements are being gathered, organized, analyzed, and validated

- all high-value services and assets have defined resilience requirements, including newly acquired assets
- asset owners are involved in the process of validating and changing requirements
- requirements changes are being communicated to custodians through formal channels
- requirements are changed as conditions dictate
- inconsistencies between requirements and requisite activities are being identified and addressed
- 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.

RRM:GG2.GP9 Objectively Evaluate Adherence

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

Elaboration:

Objective evaluation of the resilience requirements management process is intended to ensure that requirements are up-to-date and available as the basis for the organization's development, implementation, and management of strategies to protect and sustain assets and services. Therefore, objective evaluation should be focused on determining whether there is alignment between requirements and the activities being performed to meet the requirements, as well as ensuring that requirements changes are managed and controlled.

These are examples of activities to be reviewed:

- gathering and organizing resilience requirements
- obtaining commitments to requirements by owners and custodians
- maintaining changes to requirements
- maintaining traceability of requirements
- correcting inconsistencies between requirements and strategies for protecting and sustaining assets and services
- 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 any need to take corrective action

These are examples of work products to be reviewed:

- enterprise, service, and asset resilience requirements
- commitment documents
- change logs
- requirements baseline and database
- requirements traceability matrix
- documentation of inconsistencies and corrective actions
- 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 RRM:GG2.GP8 subpractice 2.)*
- contracts with external entities

RRM:GG2.GP10 Review Status with Higher Level Managers

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

Elaboration:

Assets that do not have resilience requirements, have poorly defined requirements, or have outdated requirements should be brought to the attention of higher level managers as a symptom of potential process inadequacies. In addition, inconsistencies between requirements and strategies for protecting and sustaining assets and services should also be reported. Audits of the process should be conducted regularly 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.

RRM:GG3 Institutionalize a Defined Process

Resilience requirements management is institutionalized as a defined process.

RRM:GG3.GP1 Establish a Defined Process

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

Elaboration:

The identification, tracking, and management of resilience requirements may be best performed at a level commensurate with direct ownership of the asset. Thus, this process may be often 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 management 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.

RRM:GG3.GP2 Collect Improvement Information

Collect resilience requirements management 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)
- inconsistencies arising between requirements and strategies for protecting and sustaining assets and services
- 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 requirements management process *(Refer to RRM: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.