Software Engineering Institute

CERT® Resilience Management Model, Version 1.2

Generic Goals and Practices

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

GENERIC GOALS AND PRACTICES

This document describes the generic goals and practices that the organization deploys to attain successively improving degrees of process institutionalization and capability maturity for operational resilience management. These practices exhibit the organization's commitment and ability to perform operational resilience management processes, as well as its ability to measure performance and verify implementation.

GG1 Achieve Specific Goals

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

GG1.GP1 Perform Specific Practices

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

This practice requires the organization to perform the practices, produce the work products, and deliver the services that are contained in the process definition for a process area. The organization may perform these practices in an improvised or reactive manner, and there may not be any process definition to support the performance of the practices. The degree to which the performance of practices is formalized varies from organization to organization and may be inconsistent within an organization. The success of achieving the work products and delivering the service of the practices may be directly related to the staff involved in the process.

GG2 Institutionalize a Managed Process

The process is institutionalized as a managed process.

GG2.GP1 Establish Process Governance

Establish and maintain governance over the planning and performance of the process.

This practice establishes the foundation for higher level managers' responsibility for overseeing, directing, and guiding the operational resilience management system. Higher level managers set expectations for managing operational resilience in this practice and communicate these expectations to those who are responsible as appropriate. Regular reviews of operational resilience activities are performed and reported to higher level managers for interpretation. Higher level managers make recommendations where gaps are perceived in process performance.

The behavioral expectations of higher level managers are instantiated in organizational policies that address operational resilience management, as well as in expectations for planning and performing operational resilience processes.

Higher level managers are also responsible for ensuring appropriate levels of compliance with legal, regulatory, contractual, and government obligations.

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

Subpractices

1. Establish governance over process activities.

   The organization's governance activity is expanded to include oversight over the activities and processes that the organization uses to manage operational resilience and to perform the process.

2. Develop and publish organizational policy for the process.

   Establish the organizational expectations for planning and performing the process, and communicate these expectations via policy. The policy should reflect higher level managers' objectives for the process.

GG2.GP2 Plan the Process

Establish and maintain the plan for performing the process.

In this practice, the organization determines what is needed to perform the process and to achieve the established objectives, to prepare a plan for performing the process, to prepare a process description, and to get agreement on the plan from relevant stakeholders. In some cases, this generic practice may be applied to a planning process in a particular process area; in that case, this generic practice sets an expectation that the planning process itself needs to be planned.

Establishing a plan includes documenting the plan and providing a process description, *as well as assigning ownership* of the plan with requisite authority to carry out the plan. Maintaining the plan includes changing it as necessary to reflect corrective actions, changes in requirements, or improvements.

The plan for the process should be directly influenced by the strategic and operational planning processes of the organization and reflect strategic objectives and initiatives where appropriate.

The plan for performing the process typically includes the following elements and activities:

- process description
- standards and requirements for the work products and services of the process
- specific objectives for the performance of the process
- dependencies among the activities, work products, and services of the process
- the assignment of resources (typically funding, people, and tools) needed to perform the process

- assignment of responsibility and authority
- training needed to perform and support the process
- work products to be controlled and the level of control to apply
- measurement requirements to provide insight into the performance of the process, its work products, and its services
- involvement of identified stakeholders
- activities for measuring and controlling the process
- activities for objectively evaluating the process
- activities for management review of the process and the work products

Refer to the Enterprise Focus process area for more information about creating, resourcing, and implementing a strategic resilience plan and establishing a resilience program as part of an operational resilience management system.

Refer to individual process areas for specific guidance on creating, implementing, and managing plans, where relevant.

Subpractices

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

   This plan may be a stand-alone document, embedded in a more comprehensive document, or distributed across multiple documents. In the case of the plan being distributed across multiple documents, ensure that a coherent picture of who does what is preserved.

2. Define and document the process description.

   The process description, which includes relevant standards and procedures, may be included as part of the plan for performing the process or may be included in the plan by reference.

3. Review the plan with relevant stakeholders and get their agreement.

   Review the planned process to ensure that it satisfies policy (and the requirements for governance), plans, requirements, and standards to provide assurance to stakeholders.

4. Revise the plan as necessary.

GG2.GP3 Provide Resources

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

This practice focuses on providing the resources necessary to perform the process as defined by the plan and ensuring that resources are available when needed. Resources are formally identified and assigned to process plan elements.

Resources include an adequate number of skilled staff, expense and capital funding, facilities, and tools, techniques, and methods. The interpretation of the term *adequate* depends upon many factors and can change over time.

Inadequate resources may be addressed by increasing resources or by removing requirements, constraints, and commitments.

Subpractices

1. Staff the process.

   Ensure that a sufficient and adequate level of human resources is available and appropriately skilled to perform the process.

   Staff responsible for performing process activities may be different from those responsible for evaluating the performance of the process.

   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.

   Funding must be earmarked and provided to support the goals and objectives of operational resilience management processes. Funding is an indication of higher level managers' support and sponsorship of the process.

   At a minimum, funding must be available to support proper oversight of the process. This includes (1) establishing and maintaining an appropriate internal control system for services and related assets and (2) periodic reporting of key indicators and metrics to assess process performance.

   Refer to the Financial Resource Management process area for information about budgeting for, funding, and accounting for operational resilience management processes.

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

GG2.GP4 Assign Responsibility

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

This practice ensures that there is accountability and responsibility for performing the process and ensuring the achievement of expected results throughout the life of the process. The people assigned must have the appropriate authority to act and to perform the assigned responsibilities.

Responsibility can be assigned and tracked through job descriptions, the process plan, or other means, such as performance management (goals and performance reviews).

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

Subpractices

1. Assign responsibility and authority for performing the process.

   Organizations may establish an operational resilience management process group to take responsibility for the overall operational resilience management system, including any specific processes. This group may also formally interface with higher level managers for the purpose of reporting on organizational progress against process goals as part of the governance process for operational resilience management.

2. Assign responsibility and authority for performing the specific tasks of the process.
3. Confirm that people assigned with responsibility and authority understand it and are willing and able to accept it.

GG2.GP5 Train People

Train the people performing or supporting the process as needed.

This practice ensures that the necessary staff have the skills and expertise to perform or support the process. The skills necessary to perform the process are documented in the plan and compared to the available resources. Training needs are identified to address skill gaps.

Appropriate training is provided to the staff who perform the work. Overview training is provided to those who interact with those performing the work.

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 creating an inventory of skill sets, establishing a skill set baseline, identifying required skill sets, and measuring and addressing skill deficiencies.

Subpractices

1. Identify process skill needs.
2. Identify process skill gaps based on available resources and their current skill levels.
3. Identify training opportunities to address skill gaps.
4. Provide training and review the training needs as necessary.

GG2.GP6 Control Work Products

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

The purpose of this practice is to establish and maintain the confidentiality, integrity, and availability of the designated work products of the process (or their descriptions) throughout their useful life. Work products of the process must be managed and controlled as operating conditions change and evolve.

The designated work products are specifically identified in the plan for performing the process, along with a specification of the appropriate level of control.

Different levels and types of protection and sustainment strategies are appropriate for different work products and for different points in time.

For some work products, it may be sufficient to maintain version control (i.e., the version of the process work product in use at a given time, past or present, is known, and changes are incorporated in a controlled manner). Version control is usually under the sole control of the owner of the process work product (typically an individual, group, or team).

Sometimes it may be critical for work products to be placed under formal or baseline configuration management. This type of control includes defining and establishing baselines at predetermined points. These baselines are formally reviewed and agreed upon and serve as the basis for further development and use of the process work product.

Some operational resilience work products may be categorized as sensitive and may require access controls commensurate with their level of sensitivity.

Because change control, version control, and configuration management are fundamental activities in many operational resilience management processes, this generic practice also addresses the processes and practices necessary to establish baseline work products (e.g., developing an asset database) and for performing change control on these work products as the operational environment changes and evolves.

In some cases, the management of work products is critical to an operational resilience management process and therefore is included in the specific practices of a process area. Examples of these practices can be found throughout process areas such as Access Management, Asset Definition and Management, and Incident Management and Control.

Most work products are information assets. Establishing appropriate controls for managing the confidentiality, integrity, and availability of information assets is addressed in the Knowledge and Information Management process area.

Establishing appropriate controls for managing the integrity and availability of technology assets, including configuration management of technical assets (such as software, hardware, and systems) as traditionally understood in the context of managing information technology, is addressed in the Technology Management process area.

Refer to the Resilience Requirements Development process area for information about developing protection and sustainment requirements for work products.

Refer to the Controls Management process area for information about managing the internal control system that ensures that work products are adequately protected and sustained.

GG2.GP7 Identify and Involve Relevant Stakeholders

Identify and involve the relevant stakeholders of the process as planned.

In this practice, the expected involvement of stakeholders is established, planned, and maintained during the execution of a process.

Stakeholders are involved in various activities in a process. Their roles should be considered in the process plan and could include

- planning
- decision making
- commitments
- communications
- coordination
- review
- appraisal
- requirements definition and documentation
- resolution of problems

The objective of planning stakeholder involvement is to ensure that interactions necessary to the process are accomplished without excessive numbers of affiliated groups and individuals impeding process execution.

In some process areas, the identification and inclusion of stakeholders in the process are critical to process success. In these areas, specific practices or subpractices have been included to address stakeholder involvement, particularly where processes reach extensively into the organization, such as in the Monitoring and Communications process areas.

Subpractices

1. Identify process stakeholders and their appropriate involvement.

   Relevant stakeholders are identified among the suppliers of inputs to, the users of outputs from, and the performers of activities within the process. Once the relevant stakeholders are identified, the appropriate level of their involvement in process activities is planned.

2. Communicate the list of stakeholders to planners and those responsible for process performance.

3. Involve relevant stakeholders in the process as planned.

GG2.GP8 Measure and Control the Process

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

The purpose of this practice is to perform the direct day-to-day measurement and controlling of the process. Appropriate visibility into the process is maintained so that appropriate corrective action can be taken when necessary. Measuring and controlling the process involve

establishing appropriate metrics and measuring appropriate attributes of the process or work products produced by the process. The metrics and measurements may be qualitative or quantitative as appropriate.

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

   The measures are of the process, its work products, and its services.

2. Review accomplishments and results of the process against the plan for performing the process.

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

   The reviews are intended to provide the immediate level of managers with appropriate visibility into the process. The reviews can be both periodic (for example, planned as part of a regular audit of the organization's internal control system) and event-driven.

   Process reviews are likely to concentrate on the effectiveness and efficiency of the internal control system for services and assets, as well as the satisfaction of service and asset resilience requirements.

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.

   New risks that could be introduced or affect the response plans for existing risks should be considered before any corrective action is taken. *(Refer to the Risk Management process area for more information about managing risk.)*

   Corrective actions may include the following:

   - taking remedial action to repair defective work products or services
   - changing the plan for performing the process
   - adjusting resources (people, tools, etc.)
   - negotiating changes to the established commitments
   - securing change to the requirements and objectives that have to be satisfied
   - terminating the effort

If corrective action is required, further analysis may be necessary to identify improvements to the process.

7. Track corrective action to closure.

GG2.GP9 Objectively Evaluate Adherence

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

The purpose of this practice is to provide assurance that the process is implemented as planned and adheres to its process description, standards, and procedures as evidenced through an evaluation of selected work products of the process. The evaluation must be independent; that is, those directly involved in the performance of the process cannot perform the objective evaluation or render an opinion on adherence.

Activities such as internal and external audits, post-event reviews, and capability appraisals allow the organization to have an independent and objective evaluation of the effectiveness of the risk management process, adherence to the process, and identification of areas of non-compliance.

Objectively evaluating adherence is especially important during times of stress (such as during incident response) to ensure that the organization is relying on processes and not reverting to ad hoc practices that require people and technology as their basis.

GG2.GP10 Review Status with Higher Level Managers

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

As a part of governing the operational resilience management system, higher level managers are provided with the appropriate visibility into the process.

Higher level managers include those in the organization above the immediate level of managers responsible for the process. This information is provided to help higher level managers to provide and enforce policy for the process, as well as to perform overall guidance. (This practice is not performed to help those who perform the direct day-to-day monitoring and controlling of the process.)

Different managers have different needs for information about the process. These reviews help ensure that informed decisions on the planning and performing of the process can be made. Therefore, these reviews are expected to be both periodic and event-driven.

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

GG3 Institutionalize a Defined Process

The process is institutionalized as a defined process.

GG3.GP1 Establish a Defined Process

Establish and maintain the description of a defined process.

The purpose of this generic practice is to establish and maintain a description of the process that is tailored from the organization's set of standard processes to address the needs of a specific organizational unit or line of business. The organization should have standard processes that define the specific operational resilience management capability, along with guidelines for tailoring these processes to meet the needs of a specific organizational unit or line of business, or any other organizationally defined operating division.

Managing the operational resilience management system is an enterprise concern that is typically carried out at the enterprise level, given that it must reflect the strategic and performance objectives for the organization. That said, aspects of the process must be tailorable and adaptable at the organizational unit or line of business level to ensure that appropriate process activities occur throughout the organization.

To achieve consistency of process application, the tailored definition of processes used at local levels must be consistent with and reflect the enterprise philosophy and strategy. This consistency allows the organization to track performance, bring risks within defined risk parameters, and derive benefits (e.g., efficiencies, value, and cost savings) at the enterprise level. It also ensures minimal variability as the process is performed across the enterprise, allowing for the sharing of process assets, work products, data, and learning. Otherwise, the execution of process activities at local levels will be inconsistent and variable, resulting in inefficiencies and ineffectiveness of these activities at the enterprise level.

Subpractices

1. Select from the organization's set of standard processes those processes that cover the 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.

GG3.GP2 Collect Improvement Information

Collect 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.

The purpose of this generic practice is to collect information and work products derived from planning and performing the process. This generic practice is performed so that the information and work products can be included in the organizational process assets and made available to those who are planning and performing the same or similar processes. The information and work products are stored in the organization's measurement repository and its process asset library.

Subpractices

1. Store process and work product measures in the organization's measurement repository.

   The process and work product measures are primarily those that are defined in the common set of measures for the organization's set of standard processes.

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.