Software Engineering Institute

CERT® Resilience Management Model, Version 1.2

Enterprise Focus (EF)

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

ENTERPRISE FOCUS

Enterprise

Purpose

The purpose of Enterprise Focus is to establish sponsorship, strategic planning, and governance over the operational resilience management system.

Introductory Notes

Managing operational resilience requires a vast array of skills and competencies. These skills and competencies traverse the organization and must converge to achieve and sustain a desired level of operational resilience.

Because resilience is an enterprise concern, the focus and direction for the operational resilience management system must come from the top: leadership to set direction and ethical standards, sponsorship to provide support and resources, and governance to ensure that the process is achieving its goals as expected. In addition, managing operational resilience must be aligned with and supportive of the achievement of the organization's strategic objectives. Focusing on these objectives provides the rationale for investing in resilience activities—because they enable the organization to achieve its mission.

The Enterprise Focus process area seeks to ensure that the enterprise owns the operational resilience management system and provides the necessary level of leadership and governance over the process. The strategic objectives of the organization are explicitly defined as the alignment factor for resilience plans, programs, and activities. Higher level managers provide sponsorship to ensure resilience activities are properly and adequately funded and to promote and nurture a resilience-aware culture throughout the organization. Finally, the organization's governance activities are expanded to focus directly on resilience—program objectives are set, standards for acceptable and ethical behavior are established, and the process is monitored to ensure it is achieving its goals. Higher level managers also provide input and recommendations when the operational resilience management system is not performing within established standards.

Enterprise Focus establishes the "critical few" for the organization—the high-value services that must be resilient to ensure mission achievement. This sets the focus for all operational risk-based activities in the organization. Through an enterprise focus, the direction and target for operational resilience management are established, operational risk management activities are coordinated, and actions are taken that enable the organization to perform adequately in achieving its targets.

Related Process Areas

Organizational risk drivers, risk appetite, and risk tolerance are established in the Risk Management process area.

The establishment of plans and programs to ensure service continuity is addressed in the Service Continuity process area.

The relationship between services and assets is addressed in Asset Definition and Management.

The management of compliance activities is addressed in the Compliance Management process area.

The development and achievement of resilience goals and objectives for staff are addressed in the Human Resource Management process area.

Providing awareness training for staff, both internal and external to the organization, is addressed in the Organizational Training and Awareness process area.

The Monitoring process area outlines processes for identifying, gathering, and communicating relevant data for decision-making processes.

The establishment of resilience funding needs and the allocation of funds are addressed in the Financial Resource Management process area.

Summary of Specific Goals and Practices

Goals	Practices
EF:SG1 Establish Strategic Objectives	EF:SG1.SP1 Establish Strategic Objectives
	EF:SG1.SP2 Establish Critical Success Factors
	EF:SG1.SP3 Establish Organizational Services
EF:SG2 Plan for Operational Resilience	EF:SG2.SP1 Establish an Operational Resilience Management Plan
	EF:SG2.SP2 Establish an Operational Resilience Management Program
EF:SG3 Establish Sponsorship	EF:SG3.SP1 Commit Funding for Operational Resilience Management
	EF:SG3.SP2 Promote a Resilience-Aware Culture
	EF:SG3.SP3 Sponsor Resilience Standards and Policies
EF:SG4 Provide Resilience Oversight	EF:SG4.SP1 Establish Resilience as a Governance Focus Area
	EF:SG4.SP2 Perform Resilience Oversight
	EF:SG4.SP3 Establish Corrective Actions

Specific Practices by Goal

EF:SG1 Establish Strategic Objectives

The strategic objectives of the organization are established as the foundation for the operational resilience management system.

The strategic objectives of the organization are derived from the organization's strategic planning process, which typically addresses a future time span of two to five years. The strategic objectives of the organization form the basis for operational resilience targets and activities and must be clearly documented and communicated at the organizational unit and line of business levels.

The organization's strategic objectives may be expressed in various forms. They may be articulated as organizational goals and objectives that form the basis for the performance of managers and staff. They may also be expressed in terms of critical success factors (CSFs), which complement goals and objectives by detailing the areas in which organizational performance is critical to meeting these goals and objectives.

Strategic objectives are important for the operational resilience management system because they provide a target that must be attained by services. Resilience activities must meet strategic objectives by protecting and sustaining assets and services to the extent necessary to attain these objectives. Failure to keep assets and services resilient may significantly impair the organization's ability to meet strategic objectives.

As a target for operational resilience management, the organization must clearly articulate its strategic objectives, describe its critical success factors, and identify the services that it performs that are of high value in meeting these objectives and satisfying these factors. Through these activities, the goals for operational resilience management are made clear, tangible, and achievable.

EF:SG1.SP1 Establish Strategic Objectives

Strategic objectives are identified and established as the basis for resilience activities.

Strategic objectives are the performance targets that the organization sets to accomplish its mission, vision, values, and purpose. They are decomposed into an organizational roadmap for performance so that all staff members are moving in the same direction.

Effective operational resilience ensures that the organization can reach its strategic objectives. The management of operational resilience must be specifically focused on enabling the achievement of strategic objectives and addressing a range of potential disruptions that can interrupt their achievement.

Strategic objectives range from general to specific. General objectives include mission, vision, and values, while specific objectives are goal-oriented and outline the targets the organization is attempting to reach (such as opening 100 stores in China or improving revenue by 14% in the next year). Strategic objectives emanate from the organization's strategic planning process. *(Resilience planning as part of the organization's overall strategic planning process is addressed in EF:SG2.SP1.)*

From a resilience management perspective, the identification, comprehension, and communication of the organization's strategic objectives provide essential and necessary guidance and direction for the operational resilience management system.

Typical work products

1. Organizational strategic objectives
2. Organizational mission, vision, values, and purpose statement

Subpractices

1. Identify the organization's mission, vision, values, and purpose.

   This information should be readily available in company literature such as staff handbooks and annual reports. Because some organizations are very large, this information may exist at each organizational unit or line of business level, rather than at an enterprise level.

2. Identify the organization's strategic objectives.

These objectives should be readily available in the organization's strategic plan (which may be composed at an enterprise or organizational unit or line of business level). These objectives are also typically the basis for the performance goals for staff and business partners and may be found as part of performance management activities.

EF:SG1.SP2 Establish Critical Success Factors

The critical success factors of the organization are identified and established.

Critical success factors are the limited number of areas in which the organization must consistently and effectively perform to succeed in meeting its strategic objectives. Critical success factors reflect management's implicit focus. They are areas that should receive constant and careful attention from managers. When critical success factors are identified, defined, and communicated, they represent a powerful set of criteria against which an organization can validate or align its activities, including those being performed to manage operational resilience.

Critical success factors have sources and dimensions. Sources represent the places where critical success factors originate. Because organizations are multi-dimensional, critical success factors can originate at every layer of management. In addition, because organizations typically have open borders, critical success factors can also be derived through industry affiliation or operating climate. In general, critical success factors have five sources:

- the industry in which the organization operates (e.g., financial services)
- the competitive environment or peer relationship of the organization (e.g., top 20 banks in the United States)
- the organization's operating environment (e.g., geographical location, current sociopolitical climate)
- temporal issues (e.g., weather, increase in terrorist activity)
- management's view of the organization (e.g., current priorities, budget climate)

In addition to sources, critical success factors have dimensions. Critical success factors can be internal or external (representing the extent to which the organization has span of control) or monitoring or adapting (keeping the status quo versus growing and evolving the organization). Dimensions are important because they represent the depth and breadth of critical success factors.

In essence, critical success factors establish a set of performance indicators that the operational resilience management system must contribute to achieving and form an important alignment factor between the policy-making level and the operational level of the organization.

Typical work products

1. Critical success factors of the organization
2. Critical success factors performance indicators

Subpractices

1. Collect data to support the development of critical success factors.

   Data may be collected through document review (the organization's charter, strategic plan and objectives, etc.) and interviews of key organizational managers.

2. Consolidate and analyze critical success factor data.

   Data can be developed into activity statements and developed into summary themes through affinity grouping.

3. Derive the critical success factors for the organization.

   Critical success factors can be developed for many layers of the organization. Typically, the organization has a set of enterprise-level critical success factors that influence organizational unit or line of business critical success factors, which in turn are reflected in manager- and staff-level critical success factors. Depending on the level at which an organization manages operational resilience, critical success factors may have to be developed at one or more of these levels.

   The critical success factors should represent a range of sources and dimensions.

4. Perform affinity analysis between strategic objectives and critical success factors.

   Affinity analysis documents the direct relationship between the achievement of a critical success factor and the accomplishment of a strategic objective.

5. Identify the key performance indicators to measure accomplishment of each critical success factor.

6. Monitor the accomplishment of critical success factors and take corrective action as necessary.

EF:SG1.SP3 Establish Organizational Services

The high-value services that support the accomplishment of strategic objectives are established.

The high-value services of the organization are the focus of the organization's operational resilience management activities. These services directly support the achievement of strategic objectives and therefore must be protected and sustained to the extent necessary to minimize disruption. Failure to keep these services viable and productive may result in significant inability to meet strategic objectives and, in some cases, the organization's mission.

In order to appropriately scope the organization's operational resilience management system and corresponding operational resilience management activities, the high-value services of the organization must be identified, prioritized, and communicated as a common target for success.

High-value services are fueled by organizational assets such as people, information, technology, and facilities. *(The link between high-value services and their supporting assets is established in the Asset Definition and Management process area.)*

Typical work products

1. Service profiles
2. Service repository
3. Service affinity analysis
4. Prioritized list of high-value services

Subpractices

1. Inventory organizational services and develop service repository.

   The organization should have at its disposal an inventory of standard services that represents the activities that the organization performs to achieve its mission. The inventory of services should include service profiles that describe the services in sufficient detail to capture the activities, tasks, and expected outcomes of the services and the assets that are of high value to the services. The service profile should also detail the business processes that cumulatively compose the service. A service repository should be created that is accessible by all who need to understand the organization's standard services.

   Sources of information about services include

   - strategic planning work products
   - business plans
   - industry, market, and competitive analyses
   - customer requests
   - contracts and other customer-focused documents
   - business process inventories and business process reengineering documentation
   - standard work process documentation and repositories

2. Document service attributes in a service profile.

   Service attributes help to describe services using a common language and taxonomy.

   Service attributes to consider in developing service profiles include

   - inputs to the service
   - outputs from the service
   - assets associated with or used by the service (This activity is formally performed in ADM:SG2.SP1 in the Asset Definition and Management process area.)
   - the owners and stakeholders of the service
   - related services and business processes
   - service-focused resilience requirements (This activity is formally performed in RRD:SG2.SP2 in the Resilience Requirements Development process area.)
   - expected service levels

   Service-level information may include

   - provider and user responsibilities
   - availability of the service
   - service hours and exceptions
   - anticipated service volume

- response times for service requests, incidents, and problems
- performance or quality targets
- key metrics to monitor
- reporting and escalation procedures
- consequences of failure
- variations available (such as "gold" service)

3. Perform affinity analysis between organizational services and objective measures such as strategic objectives and critical success factors.

   Affinity analysis compares the organization's standard services to the objective measures used by the organization to determine and validate the value of the services. Affinity analysis using the organization's strategic objectives and critical success factors is a means to help the organization prioritize services and to identify high-value services that must be made resilient.

4. Define high-value services from the organization's standard services repository.

   Organizationally high-value services are those that must meet their resilience requirements consistently in order to ensure that the organization can accomplish its strategic objectives and mission. These services are the focus of the resilience activities performed in the organization.

5. Revise the organization's service profiles and service repository and service levels as necessary.

   The organization must revise service profiles and the service repository as necessary to ensure that they reflect the most current information about services, particularly high-value services. Otherwise, the organization's resilience activities may be misdirected.

EF:SG2 Plan for Operational Resilience

Planning for the operational resilience management system is performed.

Managing operational resilience enables the achievement of strategic objectives and critical success factors and therefore must be specifically acknowledged and addressed at the highest levels of the organization, particularly in strategic planning performed at the enterprise level. Failing to consider operational resilience as a constraint in the development of the organization's strategic plan can result in an underappreciation of the activities, tasks, and practices that must be performed to ensure that potential barriers to achieving business objectives are identified and addressed. Proper consideration of operational resilience and its role in supporting strategic objectives *(as described in EF:SG1.SP1)* is achieved by establishing a plan and a program for the operational resilience management system.

EF:SG2.SP1 Establish an Operational Resilience Management Plan

A plan for managing operational resilience is established as the basis for the operational resilience management program.

The organization must develop and implement a plan for managing operational resilience that is based on meeting strategic objectives and

critical success factors and that considers the organization's risk tolerances and appetite. The operational resilience management plan is a part of the organization's strategic business plan that specifically addresses the actions, activities, and tasks that must be performed to reach resilience goals. The resilience plan becomes the foundation for the performance of the operational resilience management system in the organization.

Strategic business planning typically includes standard elements that describe the intentions of the organization and the means for achieving the intentions. In general, strategic plans include

- a description of the organization's vision, purpose, and values
- the organization's mission statement
- an articulation of the organization's critical success factors *(See EF:SG1.SP2.)*
- short- and long-term strategic objectives with corresponding actions, activities, and tasks to reach them
- a schedule for achieving the strategic objectives over the period of the plan (typically two to three years)

The strategic business plan sets forth the direction for the organization in the near and long term. The strategic objectives stated in the plan form the basis for the goals and objectives of everyone in the organization—from C-level executives to middle managers to staff. The actions of all staff must be commensurate with the strategic objectives in order for the organization to succeed in reaching business goals.

In much the same way, the organization must plan for success in managing operational resilience. Not only are the goals for operational resilience important, they are also critical for the organization to meet its strategic objectives. Thus, the organization must develop a resilience plan alongside its strategic business plan to detail the actions that must be taken to minimize disruptions that could draw the organization off course in achieving its strategic objectives.

Typical work products

1. Operational resilience management plan
2. Operational resilience management plan commitments

Subpractices

1. Develop the operational resilience management plan.

   The resilience plan should be developed in conjunction with the development of the organization's strategic business plan. The elements of the resilience plan should focus on the development of operational resilience objectives that are to be achieved by performing resilience activities throughout the organization and that correspond to the achievement of strategic objectives. The resilience plan should address

   - the organization's philosophy on resilience management
   - the structure of the resilience program for managing the resilience plan *(Establishing the resilience program is addressed in EF:SG2.SP2.)*

- the strategic resilience objectives
- coverage of the essential activities as described in the operational resilience management program
- linkages to the organization's plan for service continuity *(Planning for service continuity is addressed in the Service Continuity process area.)*
- roles and responsibilities for carrying out the strategic resilience objectives
- resources that will be required to meet the resilience objectives
- applicable training needs and requirements
- relevant costs or budgets associated with meeting the resilience objectives

2. Establish commitments to the plan.
3. Revise the plan and commitments on a cycle commensurate with the organization's strategic business planning process.

EF:SG2.SP2 Establish an Operational Resilience Management Program

A program is established to carry out the activities and practices of the operational resilience management plan.

The organization sets resilience program goals based on the resilience plan objectives and related program activities, tasks, and practices. The resilience program oversees and "owns" the operational resilience management system and the achievement of resilience objectives. This practice includes establishing a formal resilience program, staffing the program, assigning accountability and responsibility, providing oversight, and measuring performance.

Typical work products

1. Operational resilience program charter
2. Operational resilience program management plan

Subpractices

1. Establish the operational resilience management program.

   The operational resilience management program is typically responsible for ensuring that the strategic resilience objectives as documented in the operational resilience plan are achieved. Program management includes staffing the program, assigning accountability and responsibility to plan activities, tasks, and projects, and measuring performance. The operational resilience management program should draft a charter that describes its functions, scope, and objectives.

2. Fund the operational resilience management program.

   Funding the organization's operational resilience management program and related activities, tasks, and projects is addressed in the Financial Resource Management process area.

3. Assign resources to the operational resilience management program.

   Remember that some staff members will have explicit resilience-focused roles and responsibilities, while others will contribute to resilience processes through the execution of their job responsibilities. Typically, the operational resilience management

program will be operated by staff whose job responsibilities are resilience-focused. The organization should confirm that staff involved in carrying out the operational resilience management program have the requisite skills and training. *(Training for resilience-focused roles is addressed in the Human Resource Management process area.)*

4. Provide oversight to the operational resilience management program.

   The organization must oversee the activities of the operational resilience management program to ensure that strategic resilience objectives are being met consistently. Corrective actions must be identified and implemented when course correction is necessary. *(Governance over the operational resilience management program and process is addressed in EF:SG4.)*

5. Gather performance data on the achievement of strategic resilience objectives.

EF:SG3 Establish Sponsorship

Visible sponsorship of higher level managers for the operational resilience management system is established.

Sponsorship by higher level managers is a key factor in the success of the operational resilience management system. Sponsorship means that higher level managers take an active interest in the success of the operational resilience management system through actions such as including resilience in strategic planning, adequately funding resilience activities, communicating the importance of resilience, and providing oversight. Sponsorship also means that higher level managers are willing to invest in resilience activities and be measured on their success.

Visible sponsorship of the operational resilience management program can take many forms, such as

- approval and support for achieving strategic resilience objectives
- commitment to allocate the necessary resources (financial and human) for meeting the objectives
- visible, continued support for the resilience program (through inclusion on meeting agendas and the establishment of a resilience committee on the organization's board or leadership council)
- active encouragement of staff participation through support of goal setting and performance management for resilience
- establishing guiding principles, direction, and expectations for the organization through supporting resilience policies, guidelines, and standards
- delegation of responsibility and authority for accomplishing program objectives
- agreement to provide oversight and decisions on corrective activity

Through sponsorship, higher level managers set the tone for the organization—in essence they represent to the organization that resilience is important and is everyone's job rather than an exercise driven by external compliance or industry and regulatory obligations.

EF:SG3.SP1 Commit Funding for Operational Resilience Management

A commitment by higher level managers to fund resilience activities is established.

Budgeting is a process of allocating funds to organizational activities that support and promote strategic objectives. When resilience is considered a strategic competency, funding for resilience activities must be included as part of the organization's capital and expense funding needs rather than as an afterthought that is indirectly funded through IT activities or as needed when disruptive events occur.

Sponsorship of the operational resilience management system is made actionable by higher level managers' commitments to funding the resilience program and the accompanying activities and tasks. This requires that they commit to

- supporting the business case for operational resilience management
- including resilience needs in the funding of strategic objectives
- ensuring that resilience needs are adequately funded
- releasing funds as necessary to support the attainment of strategic resilience objectives

Sponsoring a financial commitment to resilience is different from allocating and budgeting the funds for resilience activities. *(The establishment of resilience funding needs and the allocation of funds are addressed in the Financial Resource Management process area.)*

Typical work products

1. Business case for resilience

Subpractices

1. Develop the business case for the operational resilience management program and process.

   Sponsorship of the investment in the operational resilience management system must be based on a sound business case. The investment in resilience must bring about tangible, measurable, and demonstrable value to the organization. The business case for resilience should

   - justify the investment through itemization of tangible benefits and results
   - articulate the strategic outcomes that would result from investments in resilience activities
   - articulate the potential risks and costs associated with not investing in resilience activities
   - establish that the funding necessary for resilience is appropriate and adequate
   - provide sufficient information to allow comparative evaluations of alternative actions
   - establish the accountability and commitments for the achievement of the benefits and strategic outcomes

2. Establish operational resilience management program and process funding as a regular part of the organization's strategic plan budgeting (capital and expense) exercise.
3. Approve allocation of funding to operational resilience management program and process activities.

EF:SG3.SP2 Promote a Resilience-Aware Culture

A resilience-aware culture is promoted through goal setting and achievement.

The success of enterprise-wide programs or initiatives often depends on the organization's ability to get all stakeholders (internal and external) moving in the same direction toward a common goal and for the common good. Evolving from a narrow security- or business-continuity-focused view to an operational resilience view requires significant changes in organizational structure, approach, and activities. Visible sponsorship by higher level managers is a key factor in catalyzing this type of organizational change.

Higher level managers promote a resilience-aware culture by their actions. These actions can be very broad but are typically focused on giving staff members a reason to "invest" their time and part of their job responsibilities in operational resilience management. These are some of the activities that higher level managers can perform to promote a resilience-aware culture:

- Communicate and promote the importance of resilience at all opportunities.
- Communicate the need for change based on the impact on achieving strategic objectives, and quell resistance efforts.
- Build a sponsorship alliance of higher level and middle managers to promote and sustain the message.
- Sponsor the development, implementation, and enforcement of resilience policies, standards, and guidelines. *(See EF:SG3.SP3.)*
- Sponsor the organizational training and awareness program. *(This is addressed in the Organizational Training and Awareness process area.)*
- Sponsor resilience awards and recognition programs for staff who make significant contributions to sustaining the organization's operational resilience.
- Set performance goals and objectives that focus on resilience and be willing to be measured on them.
- Keep resilience on the organizational performance scorecard of all staff.
- Provide opportunities for staff members to speak freely about resilience issues, concerns, and impediments.
- Sponsor inclusion of resilience concepts in job descriptions and in the hiring of new staff or the promotion of existing staff.
- Sponsor inclusion of resilience concepts in contracts with suppliers and business partners.

The development and achievement of resilience goals and objectives for staff are addressed in the Human Resource Management process area.

Providing awareness training for staff, both internal and external to the organization, is addressed in the Organizational Training and Awareness process area.

Typical work products

1. Resilience performance goals and objectives
2. Rewards and recognition programs

Subpractices

1. Establish a plan for visible promotion of a resilience-aware culture with appropriate success metrics.

   The plan should address the specific activities that higher level managers perform to support and promote a resilience-aware culture.

2. Establish performance management of higher level managers for resilience.

   Higher level managers should have explicit resilience goals that are reflected in the goals of middle managers and staff. Performance management activities should measure higher level managers on their ability to promote and communicate the importance of resilience programs and activities.

3. Establish rewards and recognition programs to support resilience acculturation.
4. Measure to the extent possible the level of acculturation of resilience awareness that is the direct result of sponsorship.

EF:SG3.SP3 Sponsor Resilience Standards and Policies

The development, implementation, enforcement, and management of resilience standards and policies are sponsored.

Policies establish an acceptable range of behaviors that managers intend to enforce and reinforce as a means to ensure accomplishment of common goals. Policies are unenforceable and lack effectiveness unless they are sponsored by higher level managers and higher level managers express their intention to hold stakeholders to compliance with the policies.

Polices are an expression of higher level managers' level of commitment to the operational resilience management system. Lack of policy sponsorship typically renders policies less effective as an administrative control because stakeholders may assume that the policies are not being enforced or that they are simply meant to be used as a guideline rather than a requirement.

The existence of policies, standards, and guidelines to support the operational resilience management system is considered to be a pervasive indicator of process maturity across all operational resilience management process areas. Policies are an important component of institutionalizing a managed process. *(Appropriate goals and practices related to policy development and implementation to support the operational resilience management system are generically described in GG2:GP1.)*

Typical work products

1. Policy statements from higher level managers

Subpractices

1. Establish policy statements reflecting higher level managers' commitment to managing resilience.

EF:SG4 Provide Resilience Oversight

Governance over the operational resilience management system is established and performed.

Governance is a process of providing strategic direction for the organization while ensuring that it meets its obligations, appropriately manages risk, and efficiently uses financial and human resources. From a resilience perspective, the concept of governance is extended to provide oversight over the operational resilience management system and to ensure that the process supports and sustains strategic objectives. Governance also typically includes the concepts of sponsorship (setting the managerial tone), compliance (ensuring that the organization is meeting its compliance obligations), and alignment (ensuring that processes such as those for operational resilience management align with strategic objectives).

The activities involved in governance are often confused with management activities. Governance is focused on providing oversight to the operational resilience management system, not performing or managing process tasks to completion. For example, the process of overseeing the identification, definition, and inventorying of high-value assets is a governance task, while performing these tasks is part of operational resilience process management. Effective resilience process governance means that senior leadership (which typically includes boards of directors and higher level managers) provides sponsorship and oversight to the process and provides direction and guidance on course correction when deemed necessary.

The inclusion of operational resilience as a focus area of the organization's broader governance activities is necessary to ensure that the operational resilience management system is viable, meets its goals and objectives, aligns with the organization's strategic objectives, and is performed to comply with all applicable laws and regulations. Failure to provide governance over the operational resilience management system may result in a lack of awareness of operational resilience issues and problems that may result in consequences to the organization.

Effective governance over the operational resilience management system requires the establishment of resilience as a governance focus area, processes for providing oversight and review, and a means for identifying, documenting, communicating, implementing, and monitoring corrective actions.

EF:SG4.SP1 Establish Resilience as a Governance Focus Area

Governance activities are extended to the operational resilience management system and accomplishment of the process goals.

Governance is a demonstration of the attention and sponsorship of management to the operational resilience management system. Higher level managers understand their responsibility for governing the operational

resilience management system as exhibited by their sponsorship of related processes, procedures, policies, standards, and guidelines.

Most organizations have defined governance processes. Typically, they extend to areas such as strategic planning, financial management, human resources, and audit. Increasingly, governance processes include areas such as business continuity and security—which extend to operational resilience and risk management. Governance also extends to improving and sustaining a resilience-aware culture.

Effective governance is necessary to reinforce desirable behaviors and to catalyze organizational change, particularly when there are significant barriers to organizational effectiveness. Because resilience is generally a new focus area in many organizations, a change in an organization's existing governance structure may be warranted to ensure adequate coverage of resilience and to encourage significant behavioral changes throughout the organization. In some cases, the resilience needs of the organization will compete with compliance obligations and the accomplishment of strategic objectives. Extending governance to the operational resilience management system provides an opportunity for higher level managers to resolve this conflict to the overall benefit of the organization.

Typical work products

1. Operational resilience management system governance framework
2. Committee charters for resilience governance
3. Code of conduct (addressing resilience issues)

Subpractices

1. Establish a governance framework for the operational resilience management system.

   The governance framework for operational resilience management specifies the structure for extending the governance activity to the operational resilience management system. The framework may address a wide range of resilience topics and needs, such as

   - the development of resilience committees
   - the specific inclusion of resilience topics on existing governance committees
   - the extension of resilience governance activities beyond the board of directors and higher level managers to organizational unit and line of business managers and other levels of the organizational structure
   - the recasting of committee charters to include resilience responsibilities
   - the establishment of a structure for monitoring and managing performance, including clear measures for success (This is addressed in EF:SG4.SP2.)
   - the identification and inclusion of appropriate stakeholders in the resilience governance process
   - the procedures, policies, standards, guidelines, and regulations around which governance for the operational resilience management system will be based
   - an operational-resilience-focused code of ethics

2. Assign roles and responsibilities for governance over the operational resilience management system.

   Governance must have ownership and accountability to be effective. Typically, an organization will have a board of directors or similar construct that will own the governance process and from which the governance activity will emanate. Board members or their equivalent will have specific roles in committees that extend to resilience. Extending governance to resilience activities may require the organization to extend roles and responsibilities to other higher level or middle managers deep into the organization.

3. Identify the procedures, policies, standards, guidelines, and regulations that will form the basis for resilience governance activities.

EF:SG4.SP2 Perform Resilience Oversight

Oversight is performed over the operational resilience management system for adherence to established procedures, policies, standards, guidelines, and regulations.

The governance function has responsibility to ensure that the organization's internal control system (whether financial, security, etc.) is implemented and functioning properly. A formal operational resilience management oversight committee or governance function is established with consistent and regular processes and procedures to "govern" the operational resilience management system.

The oversight function validates the operational resilience management system for adherence to established procedures, policies, standards, guidelines, and regulations. Exceptions to these foundational elements are addressed through a standard and consistent process, and corrective action feedback is provided to ensure alignment.

Even without a specific focus on resilience, governance is concerned with the continued effective operation of the organization toward its strategic objectives. To do this, governance requires the establishment of a benchmark from which it can measure performance. This includes the development or expansion of common tools such as an organizational dashboard or scorecard that includes not only typical information such as key metrics (key performance indicators, key risk indicators, and key control indicators), but also resilience-specific information (such as the ability to meet resilience requirements for high-value assets and services) to establish that the organization is on course.

Finally, auditing and monitoring are critical processes that extend to the timely oversight of the operational resilience management system. Auditing and monitoring the operational resilience management system on a regular basis enable the organization to identify and correct processes that are not meeting key metrics.

Governance activities include the responsibility for ensuring proper compliance with relevant resilience regulations and laws. *(The processes for compliance with these regulations and laws are addressed in the Compliance process area.)*

Governance relies upon timely and accurate data for decision making. *(The Monitoring process area outlines processes for identifying, gathering, and communicating relevant data for decision-making processes.)*

Typical work products

1. Governance dashboard or scorecard
2. Performance criteria (key indicators and metrics)
3. List of governance stakeholders
4. Data monitoring and collection methods
5. Audit plans and reports

Subpractices

1. Identify key governance stakeholders.

   Key governance stakeholders include those staff, internal and external, who are responsible for providing oversight over the operational resilience management system and developing and implementing corrective actions for poor performance.

2. Establish a governance dashboard or scorecard for measuring and managing operational resilience management system performance.

   A resilience dashboard or scorecard is a means to provide general information about the state of resilience in the organization and the effectiveness of the organization's operational resilience management activities. The dashboard or scorecard is populated from data that is monitored for and collected throughout the organization for the purposes of governance. Key indicators are established and monitored to determine performance. These key indicators incorporate the organization's tolerances and thresholds as well as standards and policies that provide a foundation for measurement and determination of process variation that is detrimental to the organization.

   Key indicators and metrics include

   - key performance indicators (KPI) that highlight performance against strategic objectives
   - key risk indicators (KRI) that provide risk thresholds that when crossed indicate levels of risk that may exceed the organization's risk tolerance or appetite
   - key control indicators (KCI) that provide information about the effectiveness of the internal control system, including administrative controls, process controls, and controls on information technology and related assets

3. Monitor and collect data for measuring key indicators and metrics and report on these indicators to key stakeholders.
4. Review audit reports on a regular basis for indicators of problems.
5. Establish a process for handling exceptions to the organization's acceptable behaviors.

   Not all decisions will be clear-cut, and there will be conflicting priorities. The governance framework must provide for processes to resolve these conflicts and to result in decisions that are in the best overall interest of the organization. Exceptions to

existing procedures, policies, standards, guidelines, and regulations may become an acceptable operating construct.

6. Establish reporting procedures to communicate results of measurement against indicators to governance stakeholders.
7. Provide reports on performance to governance stakeholders.

EF:SG4.SP3 Establish Corrective Actions

Corrective actions are identified to address performance issues.

The establishment of key metrics provides the organization with a means to identify performance issues and gaps that can result in an inability to achieve strategic objectives. Governance over the operational resilience management system relies upon the ability to identify these performance gaps in a timely and complete manner so that corrective actions can be taken before the organization's operational capacity is affected.

The governance function is responsible for interpreting the data collected for measurement of key metrics. Gaps in performance are analyzed and if necessary are escalated so that corrective actions can be developed and implemented.

Typical work products

1. Corrective action plans

Subpractices

1. Identify and analyze (measurements of) key indicators that do not meet established metrics.
2. Develop corrective actions to close perceived gaps.
3. Identify persons or groups responsible for implementing and managing corrective actions.

   Ensure that persons or groups accountable for implementing and managing corrective actions have the requisite skills and training.

4. Report on the success of the corrective actions to key stakeholders.

   If the corrective actions are not initially successful, additional corrective actions may have to be developed and implemented in order to provide continuing oversight.

5. Perform root-cause analysis to determine underlying causes of process variation for continuous improvement.

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 Enterprise Focus process area.

EF:GG1 Achieve Specific Goals

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

EF:GG1.GP1 Perform Specific Practices

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

Elaboration:

Practices EF:SG1.SP1 through EF:SG4.SP3 are performed to achieve the goals of the enterprise focus process.

EF:GG2 Institutionalize a Managed Process

Enterprise focus is institutionalized as a managed process.

EF:GG2.GP1 Establish Process Governance

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

Elaboration:

The Enterprise Focus process area is responsible for governing the operational resilience management system, which includes providing governance over all process area processes and practices described in the CERT Resilience Management Model. *(The practices contained in EF:SG4, Provide Resilience Oversight, describe how this is accomplished.)*

Process governance described here in EF:GG2.GP1 specifically addresses governance of the enterprise focus process. Governance of governance can be confusing and appear somewhat recursive on initial reading.

Subpractices

1. Establish governance over process activities.

   Elaboration:

   Governance over the enterprise focus process may be exhibited by

   - developing and publicizing higher level managers' objectives for the process
   - establishing a higher level officer position and steering committee to provide direct oversight of the process and to interface with higher level managers
   - chartering the formation of an operational resilience process group or similar construct to serve as the change agent for ensuring successful execution of operational resilience management system plans for all or selected process areas
   - sponsoring process policies, procedures, standards, and guidelines
   - sponsoring and providing oversight of the organization's operational resilience program, plans, and strategies
   - sponsoring and funding process activities

- regular reporting from organizational units to higher level managers on process activities and results
- creating dedicated higher level management feedback loops on decisions about the process and recommendations for improving the process
- conducting regular internal and external audits and related reporting to audit committees on process effectiveness
- 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 enterprise focus policy should address

- sponsorship for the process, including statements reflecting higher level managers' commitment to managing resilience
- establishment of strategic objectives, plans, and critical success factors of the organization as the foundation for the process
- the requirements for a strategic resilience plan and an operational resilience management program
- responsibility, authority, and ownership (roles and responsibilities[1]) for performing process activities
- proper compliance with relevant resilience-focused regulations and laws
- procedures, standards, and guidelines for
  - conducting acceptable and ethical behavior, including a code of conduct and code of ethics
  - identifying the high-value services that must be resilient to ensure mission achievement and the accomplishment of strategic objectives
  - managing and monitoring performance, including clear measures for success
- management and periodic monitoring of the status of all operational resilience management risks, which can be adjusted when needed, including capturing the potential risks and costs associated with not investing in resilience activities
- methods for measuring adherence to policy and codes, exceptions granted, and policy and code violations

EF:GG2.GP2 Plan the Process

Establish and maintain the plan for performing the enterprise focus process.

Subpractices

1. Define and document the plan for performing the 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.

[1] Roles may include the chief risk officer, chief compliance officer, chief security and/or chief information security officer, chief privacy officer, chief information officer, chief financial officer, general counsel, business unit executives and leaders, vice president of human resources/relations, vice president of public relations, etc.

EF:GG2.GP3 Provide Resources

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

Subpractices

1. Staff the process.

   These are examples of staff required to perform the enterprise focus process:

   - board members and higher level and other managers responsible for the governance of operational resilience management and ensuring that the operational resilience management system aligns with, supports, and sustains strategic objectives
   - board members and higher level and other managers responsible for ensuring that the organization meets its resilience compliance obligations
   - board members and higher level and other managers responsible for establishing policies and codes of ethics and conduct, and ensuring that they are enforced
   - security, business continuity, and IT operations officers, directors, and managers
   - team members of the operational resilience process group
   - owners and custodians of high-value services that support the accomplishment of strategic objectives
   - 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 the enterprise focus process.

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

   Elaboration:

   These are examples of tools, techniques, and methods to support the enterprise focus process:

   - methods for data collection and monitoring to ensure timely and accurate data for decision making
   - methods, techniques, and tools for making the business case for resilience and for assisting in making security governance investment decisions
   - methods and techniques for identifying key performance indicators, key risk indicators, and key control indicators (key metrics)
   - tools such as organizational dashboards or scorecards that present key metrics (including resilience-specific information) to measure and manage operational resilience process performance

- methods and techniques for deriving critical success factors and performing affinity analysis between these and the organization's strategic objectives
- methods, techniques, and tools for developing an inventory of standard services, service profiles, and a service repository
- methods and techniques for defining organizationally high-value services
- methods for promoting and nurturing a resilience-aware culture *(Refer to the Organizational Training and Awareness process area for more information about training and awareness activities.)*
- templates for committee charters
- techniques and tools for performing root-cause analysis to examine process variations for improvement

EF:GG2.GP4 Assign Responsibility

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

Elaboration:

The resilience strategic plan described in EF:SG2.SP1 addresses roles and responsibilities for carrying out strategic resilience objectives. EF:SG2.SP2 assigns accountability and responsibility for operational resilience management program activities, tasks, projects, and performance. EF:SG4.SP1 describes the responsibility of higher level managers for governing the operational resilience management system and the reflection of this in committee charters. EF:SG4.SP2 specifies governance responsibilities for ensuring proper compliance with relevant resilience regulations and laws and the role of key stakeholders in providing oversight.

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

   Elaboration:

   Responsibility and authority for performing enterprise focus process tasks can be formalized by

   - chartering documents for board committees, executive steering committees, and operational resilience process groups (or equivalent)
   - defining the roles and responsibilities in the operational resilience management strategic plan, program, and committee charters
   - developing policy specifying roles and responsibilities of board members and higher level managers for process activities
   - including process tasks and responsibility for these tasks in specific job descriptions

- including process tasks in staff performance management goals and objectives with the requisite measurement of progress against these goals

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

EF:GG2.GP5 Train People

Train the people performing or supporting the enterprise focus process as needed.

Refer to the Organizational Training and Awareness process area for more information about training the staff 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 set deficiencies.

Subpractices

1. Identify process skill needs.

   Elaboration:

   These are examples of skills required in the enterprise focus process:

   - developing, disseminating, and enforcing policy
   - establishing and managing an operational resilience process group or similar construct
   - knowledge necessary to perform the process using selected methods, techniques, and tools identified in EF:GG2.GP3 subpractice 3
   - knowledge necessary to collect, coordinate, and elevate process-specific operational risks to the risk management process
   - knowledge necessary to implement, manage, and monitor corrective action plans
   - strong communication skills for building and sustaining a resilience-aware culture

2. Identify process skill gaps based on available resources and their current skill levels.

3. Identify training opportunities to address skill gaps.

   Elaboration:

   These are examples of training topics:

   - roles and responsibilities of boards members, steering committees, and similar organizational officers and entities
   - deriving critical success factors and performing affinity analysis
   - interpreting and using decision dashboards and scorecards
   - selecting and using key performance indicators, key risk indicators, and key control indicators for measuring performance
   - using process methods, tools, and techniques, including those identified in EF:GG2.GP3 subpractice 3
   - obtaining familiarity with relevant codes of practice such as COSO or regulations such as Gramm-Leach-Bliley

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

EF:GG2.GP6 Control Work Products

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

Elaboration:

These are examples of enterprise focus work products placed under control:

- organizational strategic objectives and critical success factors
- service profiles, service repository, and the prioritized list of high-value services
- strategic resilience plan and resilience program charter and management plan
- business case for resilience
- resilience performance goals and objectives
- policy statements from board members and higher level managers
- operational resilience management system governance framework and committee charters
- governance dashboards and scorecards
- key indicators and metrics (KPIs, KRIs, KCIs)
- governance stakeholder list
- audit plans and reports
- corrective action plans
- process plan
- policies and procedures
- contracts with external entities

EF:GG2.GP7 Identify and Involve Relevant Stakeholders

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

Elaboration:

Several EF-specific practices address the involvement of stakeholders in the enterprise focus process. For example, EF:SG1.SP3 calls for identifying and documenting stakeholders of services in the service profile. EF:SG3.SP2 describes the importance of involving all stakeholders in promoting a resilience-aware culture. EF:SG4.SP1 and EF:SG4.SP2 require that stakeholders be identified and included in the operational resilience governance process. EF:SG4.SP3 requires that key stakeholders receive reports on the success of corrective actions.

Subpractices

1. Identify process stakeholders and their appropriate involvement.

   Elaboration:

   These are examples of stakeholders of the enterprise focus process:

   - higher level managers responsible for promoting a resilience-aware culture by their actions

- those responsible for sponsoring and enforcing all resilience policies, procedures, standards, and guidelines
- staff involved in providing oversight for the creation, review, and sustainment of the operational resilience management plan, program, and processes
- staff involved in providing oversight for the development and implementation of corrective actions for poor performance and the results of such actions
- those responsible for reviewing and ensuring action is taken based on key indicator and metrics reports
- owners and custodians of high-value services that support the accomplishment of strategic objectives

Stakeholders are involved in various tasks in the enterprise focus process, such as

- planning for the process, including the strategic operational resilience management plan and resilience program management plan
- making decisions that impact the process
- making commitments to process plans and activities
- communicating process plans and activities, including building and sustaining a resilience-aware culture
- managing operational risks to the process
- identifying organizational services, particularly high-value services
- managing and monitoring the performance of the operational resilience management system
- overseeing the operational resilience management system, as well as developing and implementing corrective action plans when dictated by poor performance
- 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.

EF:GG2.GP8 Measure and Control the Process

Measure and control the enterprise focus 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.

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 enterprise focus process:

- percentage of critical success factors that are on track according to plan per their key performance indicators
- percentage of organizational services for which a complete service profile has been documented in the service repository
- percentage of services determined to be high-value
- percentage of service profiles and service levels that have been reviewed within their review time frame
- percentage of resilience objectives that are being achieved according to plan
- percentage of operational resilience management plan commitments that are being met according to plan
- percentage of operational resilience management program and process activities for which adequate funds have been allocated
- percentage of operational resilience management program and process activities for which adequate staff have been allocated
- percentage of staff demonstrating resilience awareness commensurate with job description
- percentage of external entity relationships for which resilience requirements have been specified in the agreements with these entities (see also EXD)
- percentage of external entity relationships for which resilience requirements have been implemented per the agreements with these entities (see also EXD)
- percentage of higher-level managers with explicit resilience goals
- percentage of higher-level managers who are promoting and communicating resilience as measured by satisfactory performance evaluations
- percentage of acculturation of resilience awareness that is the direct result of sponsorship (by staff group, by organizational unit)
- percentage of higher-level managers that are fulfilling their commitments to manage resilience per policy as measured by satisfactory performance evaluations
- percentage of committee charters that include resilience responsibilities
- percentage of key operational resilience management roles for which responsibilities, accountabilities, and authority are assigned and required skills identified, including key governance stakeholders
- percentage of board meetings and/or designated committee meetings for which operational resilience management is on the agenda
- percentage of key metrics (KPIs, KRIs, KCIs) that are within acceptable ranges
- percentage of key indicators that are outside of acceptable ranges and for which a corrective action plan exists
- percentage of key indicators with corrective action plans where actions taken were successful in bringing indicators within acceptable ranges
- elapsed calendar time since key indicators were reported to governance stakeholders
- percentage of required internal and external audits completed and reviewed by the board or other designated oversight body
- percentage of audit findings that have been resolved

- percentage of incidents that caused damage, compromise, or loss beyond established thresholds to the organization's assets and services (categorized by asset, by service, by incident type, etc.)
- dollar amount of estimated damage or loss resulting from all incidents (categorized by asset, by service, by incident type, etc.)
- percentage of organizational units with established service continuity plan(s) for the services that require such a plan where the unit is the designated owner
- percentage of key external resilience requirements (laws, regulations, standards, etc.) for which the organization has been deemed by objective audit to be in compliance (see also COMP)
- level of capability achieved in other operational resilience management process areas
- percentage of operational resilience management policies that are met
- number of policy violations for policies related to each operational resilience management process area
- percentage of high-value assets (by asset type) for which a comprehensive strategy and internal control system have been implemented to address risks as necessary and to maintain these risks within acceptable thresholds
- number of enterprise-level risks referred to the risk management process
- percentage of CERT-RMM practices (based on a specific model scope) that are addressed by governance (EF) activities

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

   Elaboration:

   Periodic reviews of the enterprise focus process are needed to ensure that

   - operational resilience management is considered a key strategic concern and indicator
   - strategic operational resilience management activities are on track and key metrics are within acceptable ranges as demonstrated in governance dashboards or scorecards
   - operational resilience management policies are effective
   - issues, concerns, and risks in the operational resilience management system are being given a proper level of oversight
   - administrative, technical, and physical controls are operating as intended
   - controls are meeting the stated intent of the resilience requirements
   - 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.

Elaboration:

EF:SG4.SP3 specifically describes practices for developing corrective action plans when performance issues exist with key indicators and metrics (KPIs, KRIs, KCIs). In these cases, root-cause analysis is performed to identify improvements to the enterprise focus process.

7. Track corrective action to closure.

EF:GG2.GP9 Objectively Evaluate Adherence

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

Elaboration:

These are examples of activities to be reviewed:

- identification of the organization's strategic objectives and critical success factors (because they serve as the source of operational resilience requirements)
- development of service profiles, service attributes, service levels, and service resilience requirements
- selection process for high-value services
- development and revision cycles for operational resilience management plans to ensure that changes are commensurate with the organization's strategic business planning process
- sponsorship of higher level managers for the operational resilience management program to establish that the program is enacted and that regular actions occur that build and sustain a resilience-aware culture
- development and ongoing updating of the business case for resilience
- enactment of the governance framework for operational resilience management and the assignment of clear roles and responsibilities for governance over the operational resilience management system
- regular reporting of process performance to designated stakeholders
- tracking of corrective action plans and internal and external audit findings to closure

These are examples of work products to be reviewed:

- organizational strategic objectives and critical success factors
- service profiles, service repository, and the prioritized list of high-value services
- strategic resilience plan and resilience program charter and management plan
- business case for resilience
- resilience performance goals and objectives
- policy statements from higher level managers
- operational resilience management system governance framework and committee charters
- governance dashboards and scorecards
- key indicators and metrics (KPIs, KRIs, KCIs)
- governance stakeholder list

- audit plans and reports
- corrective action plans
- contracts with external entities

EF:GG2.GP10 Review Status with Higher Level Managers

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

Elaboration:

Status reporting on the enterprise focus process is likely part of the formal governance structure or may be performed through other organizational reporting requirements (such as through the chief risk officer or the chief resilience officer to an immediate superior). Audits of the process may be escalated to higher level managers and board members through the organization's audit committee of the board of directors or similar construct.

EF:GG3 Institutionalize a Defined Process

Enterprise focus is institutionalized as a defined process.

EF:GG3.GP1 Establish a Defined Process

Establish and maintain the description of a defined enterprise focus process.

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 enterprise focus 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 oversight 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.

EF:GG3.GP2 Collect Improvement Information

Collect enterprise focus 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:

- policy violations
- service profiles and repositories
- repository inconsistencies and issues
- reports on the effectiveness and weaknesses of controls
- improvements based on key indicators and metrics corrective action plans
- effectiveness of operational resilience management plans in execution
- lessons learned in post-event review of incidents and disruptions in continuity
- maintenance issues and concerns for assets and services
- conflicts and risks arising from dependencies on external entities
- resilience requirements that are not being satisfied or are being exceeded
- lessons learned in executing operational resilience management plans, in observing sponsorship actions of higher level managers, and in building a resilience-aware culture
- metrics and measurements of the viability of the process *(Refer to EF:GG2.GP8 subpractice 2.)*
- changes and trends in operating conditions, risk conditions, and the risk environment that affect operational resilience
- relevant internal and external audit reports and resolutions

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.