Software Engineering Institute

CERT® Resilience Management Model, Version 1.2

Risk Management (RISK)

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.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of Various or the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM-0003234

RISK MANAGEMENT

Enterprise

Purpose

The purpose of Risk Management is to identify, analyze, and respond to risks to organizational assets that could adversely affect the operation and delivery of services.

Introductory Notes

Risk management is a basic and essential organizational capability. The organization must identify, analyze, and respond to risk commensurate with its risk tolerances and appetite to ensure that it prevents potential disruptions that could interfere with its ability to meet its mission. At a tactical level, to accomplish this goal the organization must control operational risk—the risk that results from operating services and associated assets on a day-to-day basis. Operational risk encompasses the potential impact that could result from

- failed internal processes
- inadvertent or deliberate actions of people
- problems with systems or technology
- external events

Managing operational risk significantly influences operational resilience. The risk of disruption to any asset potentially renders associated services unable to meet their mission, hence reducing operational resilience. The organization must identify this risk, analyze it, and determine the extent to which it could affect operations. Addressing such risk requires a careful balance between strategies for protecting and sustaining assets and services while considering the cost of these strategies and the value of the assets and services to the organization.

The Risk Management process area establishes the organization’s responsibility to develop and implement an operational risk management plan and program that comprehensively and cooperatively cover the high-value assets and services of the organization. The organization explicitly establishes its risk tolerances and appetite based on its strategic drivers, market position, competitive environment, financial position, and other factors. With this appetite as a guide, risks to the assets of the organization are periodically identified, analyzed, and categorized, and response strategies are developed and implemented for those risks that the organization cannot afford to ignore. The impact of risk is considered and measured against the organization’s risk measurement criteria. Most important, the information gathered in risk assessment can be used to improve the effectiveness of strategies to protect and sustain assets and services.

All uses of “risk” in Risk Management refer to operational risk, specifically, risk to the operation and delivery of services. Other risk categories are beyond the scope of this process area.

Related Process Areas

The identification of vulnerabilities that may pose risk to the organization is performed in the Vulnerability Analysis and Resolution process area.

The development of protection strategies through the selection and implementation of controls is performed in each of the asset process areas: Environmental Control for Facility assets, Knowledge and Information Management for information assets, People Management and Human Resources Management for people assets and Technology Management for technology assets.

The development and implementation of a system of internal controls that may address risk are performed in the Controls Management process area.

The development, testing, and implementation of service continuity plans to address the consequences of realized risk are performed in the Service Continuity process area.

Summary of Specific Goals and Practices

Goals	Practices
RISK:SG1 Prepare for Risk Management	RISK:SG1.SP1 Determine Risk Sources and Categories
	RISK:SG1.SP2 Establish an Operational Risk Management Strategy
RISK:SG2 Establish Risk Parameters and Focus	RISK:SG2.SP1 Define Risk Parameters
	RISK:SG2.SP2 Establish Risk Measurement Criteria
RISK:SG3 Identify Risks	RISK:SG3.SP1 Identify Asset-Level Risks
	RISK:SG3.SP2 Identify Service-Level Risks
RISK:SG4 Analyze Risks	RISK:SG4.SP1 Evaluate Risks
	RISK:SG4.SP2 Categorize and Prioritize Risks
	RISK:SG4.SP3 Assign Risk Disposition
RISK:SG5 Address Risks	RISK:SG5.SP1 Develop Risk Response Plans
	RISK:SG5.SP2 Implement Risk Strategies and Plans
RISK:SG6 Use Risk Information to Manage Resilience	RISK:SG6.SP1 Review and Adjust Strategies to Protect Assets and Services
	RISK:SG6.SP2 Review and Adjust Strategies to Sustain Services

Specific Practices by Goal

RISK:SG1 Prepare for Risk Management

Preparation for risk management is performed.

Preparation for operational risk management requires the organization to develop and maintain a strategy for identifying, analyzing, and responding to operational risks. This strategy is documented in a risk management plan and addresses the activities that the organization performs enterprise-wide to carry out a continuous risk management program. This includes identifying the sources and types of operational risk and establishing a strategy that details the organization’s approach, activities, and objectives for managing these risks as a fundamental operational resilience management process.

RISK:SG1.SP1 Determine Risk Sources and Categories

The sources of risk to assets and services are identified and the categories of risk that are relevant to the organization are determined.

Identifying risk sources helps the organization to determine and categorize the types of operational risk that are most likely to affect day-to-day operations and to seed an organization-specific risk taxonomy that can be used as a tool for managing risk on a continuous basis as operating conditions change and evolve. The sources of risk can be both internal and external to the organization.

Categorizing operational risks provides the organization a means by which to perform advanced analysis and response activities that allow for similar types of risks to be effectively addressed.

Typical work products

1. Operational risk sources list
2. Operational risk categories list
3. Operational risk taxonomy

Subpractices

1. Determine operational risk sources.

   Risk sources are the fundamental areas of risk that can affect organizational services and associated assets while they are in operation to meet the organization's mission. Risk sources represent common areas where risks may originate. Typical internal and external sources include

   - poorly designed and executed business processes and services
   - inadvertent actions of people, such as accidental disclosures or modifications of information
   - intentional actions of people, such as insider threat and fraud
   - failure of systems to perform as intended, or risks posed by the complexity and unpredictability of interconnected systems
   - failures of technology, such as the unanticipated results of the execution of software and the failure of hardware components such as servers and telecommunications
   - external events and forces, such as natural disasters, failures of public infrastructure, and failures in the organization's supply chain

   Advance definition of specific risk sources for the organization provides a means for early identification of risk and can seed response plans that can cover a broad array of operational risks before the organization realizes the consequences of these risks.

2. Determine operational risk categories.

   Risk categories provide a means for collecting and organizing risk for ease of analysis and response. Typical operational risk categories align with the various sources of operational risk such as failed processes, actions of people, systems and technology, and external events but can be as granular as necessary for the organization to effectively manage risk. Operational risks may also align with the types of assets they are most likely to affect—risks to the availability of people, the confidentiality, integrity, and availability of information, etc.

3. Create an operational risk taxonomy.

   An organization-specific risk taxonomy is a way to collect and catalog common operational risks that the organization is subject to and must manage. The risk taxonomy is a means for communicating these risks and for developing organizational unit and line-of-business-specific response actions if operational assets and services are affected by them.

RISK:SG1.SP2 Establish an Operational Risk Management Strategy

A strategy for managing operational risk relative to strategic objectives is established and maintained.

Because of the pervasive nature of operational risk, a comprehensive operational risk management strategy is needed to ensure proper consideration of risk and the effects on operational resilience. The strategy provides a common foundation for the performance of operational risk management activities (which are typically dispersed throughout the organization) and for the collection, coordination, and elevation of operational risk to the organization’s enterprise risk management process.

Typical items addressed in an operational risk management strategy include

- the scope of operational risk management activities
- the methods to be used for operational risk identification, analysis, response, monitoring, and communication
- the sources of operational risk
- how the sources of operational risk should be organized, categorized, compared, and consolidated
- parameters for measuring and taking action on operational risks
- risk response techniques to be used, such as the development of layered administrative, technical, and physical controls and the development of service continuity plans
- definition of risk measures to monitor the status of the operational risks
- time intervals for risk monitoring and reassessment
- staff involved in operational risk management and the extent of their involvement in the activities noted above

The operational risk management strategy should be developed to facilitate the accumulation of operational risks as input to the organization’s enterprise risk management strategy and program. The strategy should be documented and communicated to all relevant stakeholders, internal and external, that are responsible for any operational risk management activity.

Typical work products

1. Operational risk management strategy

Subpractices

1. Develop and document an operational risk management strategy that aligns with the organization’s overall enterprise risk management strategy.
2. Communicate the operational risk management strategy to relevant stakeholders and obtain their commitment to the activities.

RISK:SG2 Establish Risk Parameters and Focus

Risk appetite and tolerances are identified and documented and the focus of risk management activities is established.

Risk parameters help the organization to establish a foundation for consistent risk consideration and measurement. Risk parameters reflect the organization’s stated risk appetite and tolerances and ensure that there is consistent measurement of operational risk across the organization. They provide common and consistent criteria for comparing risks and for characterizing the severity of consequences to the organization if risk is realized. This facilitates the organization’s process for prioritizing risk and for developing response strategies.

RISK:SG2.SP1 Define Risk Parameters

The organization’s risk parameters are defined.

Risk parameters provide the organization a means for consistent measurement of operational risk across the organization. The establishment of risk tolerance thresholds, in particular, reflects the organization’s level of risk adversity by providing levels of acceptable risk in each operational risk category that the organization establishes. Risk parameters also establish the organization’s philosophy on risk management—how risks will be controlled, who is authorized to accept risk on behalf of the organization, and how often and to what degree operational risk should be assessed.

Typical work products

1. Operational risk appetite
2. Operational risk thresholds
2. Risk management requirements

Subpractices

1. Define risk thresholds for each risk category.

   Risk thresholds are a management tool to determine when risk is in control or has exceeded acceptable organizational limits. They must be set for each category of operational risk that the organization establishes as a means for measuring and managing risk.

2. Establish risk management parameters.

RISK:SG2.SP2 Establish Risk Measurement Criteria

Criteria for measuring the organizational impact of realized risk are established.

A specific type of risk parameter that requires the organization's attention is risk measurement criteria. Risk measurement criteria are objective criteria that the organization uses for evaluating, categorizing, and prioritizing operational risks. Without these criteria, the organization would have a difficult time consistently gauging the potential effect that an operational risk could have on one or more important impact areas for the organization.

Typical work products

1. Organizational impact areas
2. Risk measurement criteria

Subpractices

1. Define organizational impact areas.

   Organizational impact areas identify the categories where realized risk may have meaningful and disruptive consequences. These areas typify what is important to the organization and to the accomplishment of its mission.

   These are examples of organizational impact areas:
   - reputation and customer confidence
   - financial health and stability
   - staff productivity
   - safety and health of staff and customers
   - fines and legal penalties
   - compliance with regulations

2. Prioritize impact areas for the organization.

   The prioritization of impact areas allows the organization to determine the relative importance of these areas to allow them to be used for risk prioritization and response.

3. Define and document risk measurement and evaluation criteria.

   Risk measurement and evaluation criteria provide the bounds on the severity of consequences to the organization across the organizationally defined impact areas. The consistent application of these criteria across all operational risks ensures that risks are prioritized according to organizational importance (even if they are specific to an organizational unit or line of business) and are addressed accordingly. The range of criteria can be either qualitative (high, medium, low) or quantitative (based on levels of loss, fines, number of customers lost, etc.).

4. Define and document risk likelihood.

   While risk probability may be difficult to establish for operational risks, the organization should establish parameters for risk probability that are used to further guide risk prioritization and response. These parameters can be qualitative (high, medium, or low) or quantitative (based on experience where available).

RISK:SG3 Identify Risks

Operational risks are identified.

The level and extent of operational risks to which the organization is subjected directly affect the organization's operational resilience. A key activity in managing and controlling operational resilience is the identification of operational risk and the mitigation of this risk before the organization is subjected to the consequences of realized risk.

RISK:SG3.SP1 Identify Asset-Level Risks

Operational risks that affect assets that support services are identified.

Operational risks that can affect assets such as people, information, technology, and facilities must be identified and addressed in order to actively manage the operational resilience of these assets and, more important, the services to which these assets are connected.

Risk identification is a foundational risk management activity. It requires the organization to identify and assess the types and extent of threats, vulnerabilities, and disruptive events that can pose risk to the operational capacity of assets and services. It is not an attempt to identify all operational risks, but only those that have meaning in the context of the categories of risk and the risk parameters established by the organization. Identified risks form a baseline from which a continuous risk management process can be established and managed.

There are many techniques that can be used to identify risk, such as

- using questionnaires and surveys
- interviewing vital managers and subject matter experts
- review of process controls
- using tools, techniques, and methodologies, such as information security risk assessments
- performing internal audits and performance reviews
- performing business impact analysis
- performing scenario planning and analysis
- using risk taxonomies for similar organizations and industries
- using lessons-learned databases, such as the incident knowledgebase
- reviewing vulnerability catalogs, such as the US-CERT Vulnerability Notes Database and MITRE's Common Vulnerabilities and Exposures (CVE) project

The identification of vulnerabilities that may pose risk to the organization is performed in the Vulnerability Analysis and Resolution process area. The activities performed in this process area can be used as a source for seeding a list of operational risks.

Typical work products

1. Organizational risk identification toolkit

2. List of operational risks, by asset category

Subpractices

1. Identify the tools, techniques, and methods that the organization can use to identify operational risks to organizational assets.

   Ensure that these tools, techniques, and methods are accessible to staff and that appropriate training is available.

2. Identify the operational risks (at the asset level) that can negatively impact high-value organizational services.

3. Develop risk statements.

   Develop risk statements that clearly articulate the context, conditions, and consequences of the risk.

   Risk statements should include information about

   - the asset affected (people, information, technology, or facilities)
   - a weakness or vulnerability of the asset that could be exploited
   - actors who would exploit the weakness
   - the means that an actor would use
   - the motive of the actor
   - the undesired outcome
   - resilience requirements that would be affected by the risk
   - the likelihood (if known) of the risk being realized
   - the consequences to the organization of the undesired outcome
   - the severity of the consequences (as measured by applying risk measurement criteria)

   Consequences resulting from realized risk should be described relative to the impact areas that the organization defined as part of defining risk measurement criteria. (For example, consequences should be articulated in terms of how the organization's reputation is affected, or if any fines and legal penalties result.)

4. Identify the relevant stakeholders associated with each documented risk.

RISK:SG3.SP2 Identify Service-Level Risks

Operational risks that potentially affect services are identified.

The disruption of asset productivity due to operational risk affects the ability of associated services to meet their mission. Thus, risks associated with organizational assets must be examined in the context of these services to determine if there is a potential impact on mission assurance, which in turn could affect the organization's ability to meet its mission. Examining risk in the context of services provides the organization additional information that must be considered when prioritizing risks for disposition.

The identification of high-value services is performed in the Enterprise Focus process area. The association of services to their associated assets is performed in the Asset Definition and Management process area.

Relevant practices in these process areas must be performed before operational risks can be examined in a service context.

Typical work products

1. Updated risk statements, with service context and consequences
2. List of operational risks, by service

Subpractices

1. Identify the services that are associated with each asset-specific risk statement. Update the risk statement to reflect associated services.
2. Determine the effect on the service that could result from the realization of risk at the asset level.
3. Update risk statement information to reflect service-specific consequences and the severity of the consequences due to realized risk.

RISK:SG4 Analyze Risks

Risks are analyzed to determine priority and importance.

Risk analysis is performed by the organization to determine the relative importance of each identified operational risk and is used to facilitate the organization’s risk disposition and response activities. Risk analysis helps the organization to place identified risks in the context of the organization’s risk drivers (tolerances, appetite, and measurement criteria), which further facilitates response planning.

RISK:SG4.SP1 Evaluate Risks

Risks are evaluated against risk tolerances and criteria, and the potential impact of risk is characterized.

To determine the extent of the operational risk, the consequences of the risk must be evaluated using the organization’s risk measurement criteria. Not all risks are the same for all organizations; what might be a major concern for one organization might be minor for another for many reasons, such as financial solvency, market position, cash reserves, and industry. Using the organization’s risk measurement criteria for valuation ensures that the risks that are most important to the organization’s unique operating circumstances are prioritized higher than those that do not directly impact organizational drivers.

Typical work products

1. Updated risk statements with impact valuation

Subpractices

1. Evaluate the identified risks using the defined risk parameters and risk measurement criteria.

   Each risk is evaluated and assigned values in accordance with the defined risk parameters and risk measurement criteria. (These include likelihood, consequence, consequence severity, and thresholds.) The organization may weigh the valuation of the risks by adjusting for the priority of impact areas (reputation, finance, etc.) that it established as part of the risk measurement criteria. This will ensure that impact areas of most importance to the organization will influence more strongly which risks are prioritized higher for response. The organization can further influence the prioritization by applying a probability factor, if known.

2. Assign a valuation to each risk statement.

   The valuation can be qualitative (high, medium, or low) or can be a quantitative relative risk score that combines likelihood, impact area weighting, and consequence value. The valuation assigned to the risk statement will be used as a factor in deciding what to do with the risk.

RISK:SG4.SP2 Categorize and Prioritize Risks

Risks are categorized and prioritized relative to risk parameters.

Categorizing operational risks can aid significantly in helping the organization to prioritize these risks for disposition. This allows the organization to view risks according to their source, taxonomy, or other commonality, which may provide insight into disposition strategies at an aggregate level. It can also facilitate further analysis and effectively streamline the risk response process, resulting in more effective protection and sustainment strategies that cover a range of potential risks.

Typical work products

1. List of risks, with categorization and prioritization

Subpractices

1. Categorize and group risks according to the defined risk categories.

   Risks are categorized into defined risk categories or other forms of categorization. This may result in merging similar risk statements or eliminating risk statements. Related risks are identified and grouped for efficient handling, and the cause-and-effect relationship between related risks is identified.

2. Prioritize risks to support disposition.

   A relative priority is determined for each risk statement (or merged risk statements) based on the assigned risk valuation. The intent of prioritization is to determine the risks that most need attention because of their potential to affect operational resilience.

RISK:SG4.SP3 Develop Risk Disposition Strategy

The strategy for disposition of each identified risk is established and maintained.

An important part of risk management is to determine a strategy for each identified risk and to implement actions to carry out the strategy. Strategy development begins with assigning a risk disposition to each risk, that is, a statement of the organization’s intention for addressing the risk.

Risk dispositions can vary widely across organizations but typically include

- risk avoidance—altering operations to avoid the risk while still providing the essential service

- risk acceptance—acknowledgment of the risk but consciously not taking any action (in essence, accepting the potential consequences of the risk)
- risk monitoring—performing further research and deferring action on the risk until the need to address the risk is apparent
- risk transfer—assigning the risk to a willing and able entity
- risk mitigation—taking active steps to minimize the risk

Because risk can rarely be eliminated, the organization must actively seek to monitor the disposition of known risks to ensure that risk conditions do not warrant changes in the assigned disposition.

Typical work products

1. List of risks, with risk dispositions
2. List of prioritized risks

Subpractices

1. Assign a risk disposition to each risk statement based on risk valuation and prioritization.

   A risk disposition is assigned to each risk statement or group of statements. The organization must establish a range of acceptable and consistent risk dispositions and their definitions.

   Possible risk dispositions include

   - avoid
   - accept
   - monitor
   - research or defer
   - transfer
   - mitigate

   Risks that are to be accepted must be approved by a sufficient level of organizational management that accepts responsibility and authority for the potential impact on operational resilience that could result. For risks that are to be transferred, there must be a clear and willing organization or person able to accept the risk. Risks that are to be researched or deferred must be carefully examined to ensure that delaying response will not result in the realization of the risk or effects on operational resilience.

2. Obtain approval for the proposed disposition of each risk, particularly risks that are not going to be mitigated.
3. Develop a plan to carry out the proposed risk disposition.
4. Monitor the risk and the risk strategy on a regular basis to ensure that the risk does not pose additional threat to the organization.

   Continuous risk management requires that the organization periodically review identified risks to ensure that they have been minimized or that changes in the risk environment do not warrant changes in the risk disposition.

RISK:SG5 Address Risks

Risks to assets and services are addressed to prevent disruption of operational resilience.

Risk response involves the development of strategies that seek to minimize the risk to an acceptable level. This includes actions to

- reduce the likelihood (probability) of the vulnerability or threat and resulting risk
- minimize exposure to the vulnerability or threat from which the risk arises
- develop service continuity plans that would keep an asset or service in production if affected by realized risk
- develop recovery and restoration plans to address the consequences of realized risk

An organization may address risks through any combination of these actions depending on the affected assets and services, their value to the organization, and the cost of the protection and sustainment strategies versus the value of the assets and services. Response may also involve revisiting resilience requirements, improving controls, and improving strategies to sustain assets and services.

Risk response requires the organization to perform two distinct actions: (1) develop risk response plans and (2) implement and monitor these plans for effectiveness.

The development of protection strategies through the selection and implementation of controls is performed in each of the asset process areas: Environmental Control for Facility assets, Knowledge and Information Management for information assets, People Management and Human Resources Management for people assets and Technology Management for technology assets. The development of a system of internal controls is performed in the Controls Management process area. The development and implementation of service continuity plans are performed in the Service Continuity process area.

RISK:SG5.SP1 Develop Risk Response Plans

Risk response plans are developed.

When the consequences of risk exceed the organization’s risk thresholds and are determined to be unacceptable, the organization must act to address risk to the extent possible.

Addressing risk requires the development of response strategies that may include a wide range of activities. In some cases, risk response will require adjustments to current strategies for protecting and sustaining assets and services. In other cases, the organization will find itself designing and implementing new controls and developing and implementing new service continuity plans. In addition, because not all risk can be mitigated, the organization must be able to address residual risk—the risk that remains and is accepted by the organization after response plans are implemented. This risk must be analyzed and determined to be acceptable before the risk response plan is in place.

Typical work products

1. Risk response plans

2. List of those responsible for addressing and tracking risk

Subpractices

1. Develop risk response plans for all risks that have a “mitigate” or “control” disposition.

   Developing risk response plans is an extensive activity that will vary by organization. There are some common elements of risk response plans that should be considered for all plans:

   - how the threat or vulnerability will be reduced
   - the actions that will prevent or limit an actor from exploiting a threat or vulnerability
   - the controls that will have to be implemented or updated to reduce exposure, including an articulation of administrative, physical, and technical controls
   - the service continuity plans that would be used to reduce the impact of consequences should risk be realized
   - the staff who are responsible for implementing and monitoring the response plan
   - the cost of the plan, and a cost-benefit analysis that demonstrates the value of the plan commensurate with the value of the related assets and services or avoidance of consequences
   - the implementation specifics of the plan (when, where, how)
   - the residual risk that would not be addressed by the plan

2. Validate the risk response plans by comparing them to existing strategies to protect and sustain assets and services.

   The risk response plans should be validated against the current protection strategies and controls in place to protect assets and services and the sustainment strategies and service continuity plans available to manage the consequences of risk. Any gaps should be reflected in the plan. *(Improving protection and sustainment activities as a result of risk management activities is addressed in RISK:SG6.)*

3. Identify the person or group responsible for each risk response plan and ensure they have the authority to act and the proper level of skills and training to implement and monitor the plan.

4. Address residual risk.

   Residual risk must be specifically accepted, deferred, or transferred. Otherwise, it must be considered as a risk that must be addressed, requiring reconsideration of the risk response plan.

RISK:SG5.SP2 Implement Risk Strategies and Plans

Risk strategies and response plans are implemented and monitored.

Effective management and control of risk require the organization to monitor risk and the status of risk strategies. Because the operational environment is constantly changing, risks identified and addressed may have to be revisited, and a new disposition and strategy may have to be developed.

The risk management strategy defines the intervals at which the status of risk strategies must be revisited. This may align with the organization's regular intervals of risk identification, or it may be an activity that is performed independently of risk identification.

The implementation of risk strategies requires the monitoring of risks according to their disposition and the implementation and monitoring of risk response plans.

Typical work products

1. Risk response plans
2. Updated list of risks, with current status

Subpractices

1. Monitor risk status.

   The disposition of risks that are not being mitigated or otherwise controlled in some way must be periodically assessed and revised as necessary. Some risks may, under future circumstances, require the development of a response plan.

2. Provide a method for tracking open risks to closure.
3. Implement the risk response plans and provide a method to monitor the effectiveness of these plans.
4. Provide continued commitment of resources for each plan to allow successful execution of the risk management activities.
5. Collect performance measures on the risk management process.

RISK:SG6 Use Risk Information to Manage Resilience

Information gathered from identified and realized risk is used to improve the operational resilience management system.

Because of the direct effect of risk management on operational resilience, continuous risk management processes can be a force in improving and sustaining operational resilience. What is learned in risk identification, assessment, and response directly affects existing strategies for protecting and sustaining assets and services, which can benefit from the risk management process.

To use risk information to manage operational resilience, the organization must directly use risk information as input to validating the effectiveness of current protection and sustainment strategies and to improve these strategies based on an understanding of risk.

RISK:SG6.SP1 Review and Adjust Strategies to Protect Assets and Services

Protection strategies implemented to protect assets and services from risk are evaluated and updated as required based on risk information.

The controls and other strategies that an organization uses to protect assets and services from operational risk are typically based on resilience requirements. However, considerations of risk as identified in the risk management process can result in improvements and enhancements that cannot be envisioned through translation of resilience requirements into an internal control system. Thus, improving and sustaining the organization's operational resilience is also dependent upon using the lessons learned in risk management to improve protection by implementing missing controls, updating existing controls, or considering other protection strategies to address new and emerging risks.

Typical work products

1. Protection strategies for high value assets and services
2. Results of business impact analysis or risk assessment
3. Risk register
4. Current risk profile for high-value assets and services
5. Controls list (of controls that have to be fixed, revised, or developed)

Subpractices

1. Compare risk response plans to existing protection strategies for affected assets and services.

   Comparing risk response plans to existing protection strategies and controls may help the organization to identify strategies and controls that are not working properly, that have to be updated or revised, and that may be missing.

2. Revise existing strategies and controls or develop and implement additional protection mechanisms that are necessary to address risks.

RISK:SG6.SP2 Review and Adjust Strategies to Sustain Services

Sustainment strategies are developed to ensure services are sustained and plans are evaluated and updated as required based on risk information.

Just as the protection strategies and associated controls can be improved to prevent risk realization, the organization's ability to sustain assets and services in light of realized risk can be improved through what is learned in the risk management cycle. This can result in the identification of inadequate sustainment plans, strategies that have to be revised or updated, or missing strategies. Validating service continuity plans through identified risks also provides another means to ensure effective sustainment in covering a range of possible threats and operational risks.

Typical work products

1. Sustainment strategies and plans for high-value assets and services
2. Results of business impact analysis or risk assessment
3. Risk register
4. Current risk profile for high-value assets and services
5. Sustainment strategies or service continuity plan list (of plans that have to be fixed, revised, or developed)

Subpractices

1. Compare risk response plans to existing sustainment strategies and service continuity plans for affected assets and services.

   Comparing risk response plans to existing sustainment strategies will identify items that may be inadequate, in need of updating and revision, or missing.

2. Revise existing sustainment strategies and service continuity plans or develop and implement additional plans or other sustainment mechanisms that are necessary to address risks.

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 Risk Management process area.

RISK:GG1 Achieve Specific Goals

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

RISK:GG1.GP1 Perform Specific Practices

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

Elaboration:

Specific practices RISK:SG1.SP1 through RISK:SG6.SP2 are performed to achieve the goals of the risk management process.

RISK:GG2 Institutionalize a Managed Process

Risk management is institutionalized as a managed process.

RISK:GG2.GP1 Establish Process Governance

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

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

Subpractices

1. Establish governance over process activities.

   Elaboration:

   Governance over the risk management processes may be exhibited by

   - developing and publicizing higher level managers’ objectives and requirements for the process

- establishing a higher level risk officer position to provide direct oversight of the process and to interface with higher level managers
- sponsoring and providing oversight of process policies, procedures, standards, and guidelines, including establishing risk tolerances, thresholds, and evaluation criteria
- sponsoring and providing oversight of the organization's risk management program, plans, and strategies, including the process plan
- sponsoring and funding process activities
- ensuring that high-priority risks referred to the process from other operational resilience processes are addressed in a timely manner
- regular reporting from organizational units to higher level managers on process activities and results
- implementing a risk management steering committee
- making higher level managers aware of applicable compliance obligations related to managing risk, and regularly reporting on the organization's satisfaction of these obligations to higher level managers
- verifying that the process supports strategic resilience objectives and is focused on assets and services that are of the highest relative value in meeting strategic objectives
- 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 appropriate 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 risk management policy should address

- responsibility, authority, and ownership for performing process activities
- procedures, standards, and guidelines for
    - identifying risk sources and categories of risk
    - defining risk parameters (such as risk tolerance thresholds) and risk measurement criteria
    - assigning risk priorities based on risk valuation
    - assigning risk dispositions
    - developing risk response plans
- periodically monitoring the status of all risks and adjusting as necessary
- methods for measuring adherence to policy, exceptions granted, and policy violations

RISK:GG2.GP2 Plan the Process

Establish and maintain the plan for performing the risk management process.

Elaboration:

The plan for the risk management 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 the risk management process should not be confused with a risk management plan or plans for responding to risk as described in RISK:SG5.SP1. The plan for the risk management process details how the organization will perform risk management, including the development of risk management and response plans.

Subpractices

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

   Elaboration:

   Special consideration in the plan may have to be given to the adequacy of the internal control system for information, technology, facility, and people assets and the services they support.

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

RISK:GG2.GP3 Provide Resources

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

Subpractices

1. Staff the process.

   Elaboration:

   It should be noted that this generic goal related to risk management refers to staffing the risk management process plan, not the individual risk management response plans. *(Assigning resources to risk management response plans is described in RISK:SG5.SP2.)*

   These are examples of staff required to perform the risk management process. Such people may include organizational unit managers, line of business managers, project managers, and asset and service owners and custodians.

   - the chief risk officer or equivalent
   - a risk management steering council, group, or process group
   - staff responsible for
     - identifying operational risk sources and categories
     - identifying and assessing operational risks, including risks identified by the process and other resilience management processes

  - business impact analysis
  - scenario planning and analysis
  - assigning risk disposition to risk statements based on risk valuation and prioritization
  - developing risk response plans and implementing these plans, including accepting, deferring, or transferring residual risk
  - monitoring and tracking risks to closure
  - managing external entities that have contractual obligations for risk management activities
- higher level managers responsible for defining risk parameters, including risk tolerance thresholds, authorization for levels of risk acceptance, organizational impact areas and priorities, and risk measurement criteria
- staff skilled in interview techniques and the use of questionnaires and surveys
- vital managers and subject matter experts
- external entities involved in process activities and in assessing risk on outsourced functions
- 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 risk management.

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

Elaboration:

These are examples of tools, techniques, and methods to support the risk management process:

- methods and tools for determining, documenting, and communicating risk sources, categories, parameters, and measurement criteria
- methods for operational risk identification, analysis, response, monitoring, and communication with respect to identified assets and services *(Techniques for risk identification are described in RISK:SG3.SP1.)*
- techniques for risk assessment, including interview techniques, questionnaires, and surveys
- methods, techniques, and tools for business impact analysis
- tools for scenario planning and analysis
- tools for developing risk response plans
- templates for documenting risk response plans
- methods for tracking open risks to closure
- methods for keeping stakeholders apprised of the current status of open risks

- methods for monitoring the effectiveness of risk response plans
- tools, techniques, and methods for version control of risk response plans

RISK:GG2.GP4 Assign Responsibility

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

Elaboration:

RISK:SG4.SP3 describes the level of management responsibility and authority required based on risk disposition but does not directly address responsibility and authority for carrying out the risk management process plan.

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

Subpractices

1. Assign responsibility and authority for performing the process.

   Elaboration:

   Organizations may establish a risk officer, a risk management group, or a risk management process group to take responsibility for the overall risk management process. This group may also formally interface with higher level managers for the purposes of reporting on organizational progress against risk management process goals as part of the governance process.

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

   Elaboration:

   Responsibility and authority for performing risk management tasks can be formalized by

   - defining roles and responsibilities in the process plan to include roles responsible for addressing and tracking risk
   - including process tasks and responsibility for these tasks in specific job descriptions, particularly for those staff who own high-value organizational assets
   - developing policy requiring organizational unit managers, line of business managers, project managers, and asset and service owners and custodians to participate in and derive benefit from the process for assets and services under their ownership or custodianship
   - including process activities in staff performance management goals and objectives, with requisite measurement of progress against these goals
   - developing and implementing contractual instruments (including service level agreements) with external entities to establish responsibility and authority for performing process tasks on outsourced functions
   - including process tasks in measuring performance of external entities against contractual instruments

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

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

RISK:GG2.GP5 Train People

Train the people performing or supporting the risk management process as needed.

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

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

Subpractices

1. Identify process skill needs.

Elaboration:

These are examples of skills required in the risk management process:

- knowledge of tools, techniques, and methods that can be used to identify, analyze, mitigate, and monitor operational risks to organizational assets and services, including those identified in RISK:GG2.GP3 subpractice 3
- knowledge necessary to develop, implement, and monitor risk response plans
- knowledge necessary to collect, coordinate, and elevate operational risks to the organization's enterprise risk management process
- strong communication skills for conveying the operational risk management strategy, identified risks, and response plans to higher level managers and key stakeholders so as to obtain their commitment

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

3. Identify training opportunities to address skill gaps.

Elaboration:

Certification training is an effective way to improve risk management skills and attain competency. While operational risk management certifications are not widespread, GIAC (Global Information Assurance Certification) does offer a Certified Project Manager Certification that includes risk management of IT projects and application development. The Information Systems Examination Board (ISEB) of the British Computer Society offers a Practitioner Certificate in Information Risk Management.

These are examples of training topics:

- risk management concepts and activities (e.g., risk identification, evaluation, monitoring, mitigation techniques, and other responses to address risk)
- selection of protection strategies and measures for addressing risk
- establishing risk tolerance, threshold, and evaluation criteria
- developing risk management strategy

- establishing and managing a continuous process
- using process tools and techniques
- working with external entities that have responsibility for process activities and for assessing risk on outsourced functions
- using process methods, tools, and techniques, including those identified in RISK:GG2.GP3 subpractice 3

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

RISK:GG2.GP6 Control Work Products

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

Elaboration:

These are examples of risk management work products placed under control:

- operational risk source list, risk categories list, and taxonomy
- operational risk management plan and strategy
- operational risk parameters and measurement criteria
- list of operational risks by asset category and service with prioritization, risk disposition, responses, and current status
- risk statements with impact valuation
- risk response plans
- process plan
- policies and procedures
- contracts with external entities

RISK:GG2.GP7 Identify and Involve Relevant Stakeholders

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

Elaboration:

Several RISK-specific practices address the involvement of stakeholders in the risk management process. For example, RISK:SG1.SP2 addresses the communication of the operational risk management strategy to relevant stakeholders. RISK:SG3.SP1 calls for identifying relevant stakeholders associated with each documented risk.

Subpractices

1. Identify process stakeholders and their appropriate involvement.

Elaboration:

These are examples of stakeholders of the risk management process:

- organizational unit managers, line of business managers, project managers, and business process owners
- owners of identified assets and services (for which plans to manage risks must be developed)
- custodians of identified assets and services (who may need to execute or participate in plans)

- staff involved in identifying, analyzing, mitigating, and controlling risks to assets and services (such as information technology, human resources, legal, and compliance staff)
- staff involved in reviewing and adjusting strategies to protect and sustain assets and services
- the owner of any resilience management process who has referred risks to the process
- risk owners
- risk response plan owners

Stakeholders are involved in various tasks in the risk management process, such as

- planning for the process
- making decisions about the process
- making commitments to process plans and activities
- communicating process plans and activities
- coordinating process activities
- developing process parameters
- identifying risk
- analyzing risk (particularly where technical expertise is required), including assessing the adequacy of the internal control system
- developing and implementing risk response plans
- reviewing and appraising the effectiveness of process activities
- establishing requirements for the process
- 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.

RISK:GG2.GP8 Measure and Control the Process

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

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

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

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

Subpractices

1. Measure actual performance against the plan for performing the process.

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

Elaboration:

These are examples of metrics for the risk management process:

- number of internal operational risk sources identified
- number of external operational risk sources identified
- number of operational risk sources that are not addressed by process policies or other response activities
- number of risk categories defined
- elapsed time since validation of risk categories performed
- percentage of repeat audit findings related to operational risk management
- number of operational risks referred to the organization’s enterprise risk management process
- number of risk parameters defined
- elapsed time since validation of risk parameters performed
- number of risk criteria defined
- elapsed time since validation of risk criteria performed
- elapsed time since risk assessment performed
- elapsed time since business impact analysis performed
- percentage of assets for which some form of risk assessment has not been performed and documented (per policy or other guideline) within the specified timeframe
- percentage of services for which some form of risk assessment of associated assets has not been performed and documented (per policy or other guideline)
- confidence factor that all risks that need to be identified have been identified
- change in number of identified risks that exceed risk parameters and measurement criteria
- percentage of risks for which the impact (refer to RISK:SG2.SP2) has not been characterized (qualitative, quantitative)
- percentage of risks that have not been categorized and prioritized
- percentage of risks that have been characterized as “high” impact according to risk parameters (refer to RISK:SG2)
- percentage of risks that exceed established risk parameters and measurement criteria, by risk category
- percentage of risks that do not have a documented and approved risk disposition
- percentage of risks that have not been assigned to a responsible party for action, tracking, and closure
- percentage of previously identified risks that have converted from any other risk disposition to a risk disposition of “mitigate”
- percentage of risks with a disposition of “mitigate” that do not have a defined response plan
- percentage of assets for which a response plan has been implemented to mitigate risks as necessary and to maintain these risks within acceptable risk parameters
- percentage of services with an implemented response plan

- percentage of risks with a “mitigate” disposition with mitigations that are not yet started
- percentage of risks with a “mitigate” disposition with mitigations that are in progress (vs. completely implemented)
- percentage of risks with a “mitigate” disposition that are not effectively mitigated by their response plans
- percentage of open risks that have not been tracked to closure
- percentage of risks with a disposition of “mitigate” that have a defined mitigation plan but whose status is not regularly reported (per policy or other guideline)
- percentage of realized risks that exceed established risk parameters
- elapsed time since risks with the following dispositions were last reviewed and disposition confirmed: avoid, accept, monitor, research or defer, transfer

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

Elaboration:

Reviews of the risk management process may result from periodic examination or post-event audits that seek to identify problems that must be corrected. Elevating the results of these examinations to managers provides an opportunity to correct risk management process deficiencies and to make managers aware of variations in the risk management process that not only have localized impact but may also affect the organization’s resilience as a whole.

Periodic reviews of the risk management process are needed to ensure that

- actions requiring management involvement are elevated in a timely manner
- the performance of process activities is being monitored and regularly reported
- key measures are within acceptable ranges as demonstrated in governance dashboards or scorecards and financial reports
- administrative, technical, and physical controls are operating as intended to protect assets and services from risk
- actions requiring management involvement are elevated in a timely manner
- actions resulting from internal and external audits are being closed in a timely manner
- work products accurately reflect what is essential for managing operational risk to ensure mission success, or are corrected or modified if necessary.

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

Elaboration:

Deviations from the risk management plan may occur because operational risks for assets and services vary widely, and thus the response to these risks may require process deviations. The organization must determine if the deviations are appropriate given the risk parameters and whether the deviation will result in an impact on operational resilience.

In addition, deviations from the risk management plan may occur when organizational units fail to follow the enterprise-sponsored process. These deviations may affect the operational resilience of the organizational unit's services but may also have a cascading effect on enterprise operational resilience objectives.

5. Identify problems in the plan for performing the process and in the execution of the process.
6. Take corrective action when requirements and objectives are not being satisfied, when issues are identified, or when progress differs significantly from the plan for performing the process.
7. Track corrective action to closure.

RISK:GG2.GP9 Objectively Evaluate Adherence

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

Elaboration:

These are examples of activities to be reviewed:

- risk planning, including establishing tolerances, thresholds, and other parameters
- risk assessment, including risk identification, analysis, and prioritization
- risk response planning
- risk monitoring
- use of risk-based information for improving strategies for protecting and sustaining assets and services
- assignment of responsibility, accountability, and authority for process activities
- determining the adequacy of process reports and reviews in informing decision makers regarding the performance of operational resilience management activities and the need to take corrective action, if any

These are examples of work products to be reviewed:

- process plan and policies
- risk management plans and risk response plans
- operational risk sources, risk categories, and risk taxonomy
- operational risk management strategy
- risk parameters, impact areas, and measurement criteria
- operational risks by asset category and service
- risk statements
- risk dispositions and priorities
- risk owners (those responsible for each risk with the authority to act)
- list of controls necessary to address risks
- process methods, techniques, and tools
- metrics for the process *(Refer to RISK:GG2.GP9 subpractice 2.)*
- contracts with external entities

RISK:GG2.GP10 Review Status with Higher Level Managers

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

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

RISK:GG3 Institutionalize as a Defined Process

Risk management is institutionalized as a defined process.

RISK:GG3.GP1 Establish a Defined Process

Establish and maintain the description of a defined risk management 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 risk management process and best meet the needs of the organizational unit or line of business.
2. Establish the defined process by tailoring the selected processes according to the organization’s tailoring guidelines.
3. Ensure that the organization’s process objectives are appropriately addressed in the defined process, and ensure that process governance extends to the tailored processes.
4. Document the defined process and the records of the tailoring.
5. Revise the description of the defined process as necessary.

RISK:GG3.GP2 Collect Improvement Information

Collect risk management work products, measures, measurement results, and improvement information derived from planning and performing the process to support future use and improvement of the organization’s processes and process assets.

Elaboration:

These are examples of improvement work products and information:

- metrics and measurements of the viability of the process *(Refer to RISK:GG2.GP8 subpractice 2.)*
- changes and trends in operating conditions that affect risk sources and categories
- changes in risk conditions and the risk environment that affect risk parameters, measurement criteria, or risk dispositions

- lessons learned in post-event review of continuity exercises, incidents, and disruptions in continuity, particularly those that result in losses or compromises that exceed risk parameters and measurement criteria
- process lessons learned that can be applied to improve operational resilience management performance and internal controls
- issues with the risk planning, identification, analysis, prioritization, overall assessment, mitigation, and monitoring processes
- lessons learned from both successfully and unsuccessfully addressing identified risks
- risk response plan costs and benefits for future return on investment analysis
- resilience requirements that are not being satisfied or are being exceeded

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

Subpractices

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