Software Engineering Institute

CERT® Resilience Management Model, Version 1.2

Monitoring (MON)

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/

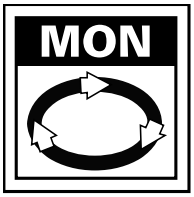
Carnegie Mellon

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

MONITORING

Process



Purpose

The purpose of Monitoring is to collect, record, and distribute information about the operational resilience management system to the organization on a timely basis.

Introductory Notes

Monitoring is an enterprise-wide activity that the organization uses to "take the pulse" of its day-to-day operations and, in particular, its operational resilience management processes. The proactive discovery and analysis of data related to operational activities ensure that stakeholders have the information needed to make decisions before, during, or after a disruption occurs. Monitoring provides the information that the organization needs to determine whether it is being subjected to threats and vulnerabilities that require action to prevent organizational impact. Monitoring also provides valuable information about operating conditions that could indicate a need for active organizational involvement.

Many operational resilience management processes implicitly require monitoring capacities in order to achieve higher maturity goals. For example, monitoring provides data about changes in the user environment that can result in necessary changes in access privileges. Effective monitoring also informs the organization when new vulnerabilities emerge (either inside or outside of the organization) or when events or incidents require the organization's attention. This information may require the organization to change its strategy, improve control selection, implementation, and management, or improve the details of its service continuity plans. In addition, the organization's compliance process—which is by nature data-intensive—benefits from monitoring activities by receiving up-to-date information that can be important to compliance activities. In essence, monitoring is a core capability that the organization must master in order to achieve the situational awareness necessary to sustain a level of adequate resilience.

Monitoring is also a data collection activity that allows the organization to measure process effectiveness across resilience capabilities. For example, through monitoring, the organization can determine whether its resilience goals are being met. It can also ascertain whether its security activities are effective and producing the intended results. Monitoring is one way that the organization collects necessary data (and invokes a vital feedback loop) to know how well it is performing in managing the operational resilience management system.

The Monitoring process area focuses on the activities the organization performs to collect, record, and distribute relevant data to the organization for the purposes of managing resilience and providing data for measuring process effectiveness. To do this, the organization must establish the stakeholders of the monitoring process (i.e., those that have a need for timely information about resilience activities) and determine their requirements and needs. The organization must also determine its monitoring

requirements for managing both operational resilience and the operational resilience management system and ensure that resources have been assigned to meet these requirements. Data collection, recording, and distribution take organizational resources. Thus, the organization must consider and implement an infrastructure that supports and enables its monitoring needs and capabilities. Finally, the organization must collect, organize, record, and make available the necessary information in a manner that is timely and accurate and that ensures data confidentiality, integrity, and availability.

Related Process Areas

The Monitoring process area provides essential data necessary to manage several operational resilience management processes. These processes include Incident Management and Control, Vulnerability Analysis and Resolution, Risk Management, and others. From a process improvement perspective, all operational resilience management process areas may rely upon data collected and distributed through monitoring practices as described in this process area.

Resilience communications are addressed in the Communications Management process area.

Summary of Specific Goals and Practices

Goals	Practices
MON:SG1 Establish and Maintain a Monitoring Program	MON:SG1.SP1 Establish a Monitoring Program
	MON:SG1.SP2 Identify Stakeholders
	MON:SG1.SP3 Establish Monitoring Requirements
	MON:SG1.SP4 Analyze and Prioritize Monitoring Requirements
MON:SG2 Perform Monitoring	MON:SG2.SP1 Establish and Maintain Monitoring Infrastructure
	MON:SG2.SP2 Establish Collection Standards and Guidelines
	MON:SG2.SP3 Collect and Record Information
	MON:SG2.SP4 Distribute Information

Specific Practices by Goal

MON:SG1 Establish and Maintain a Monitoring Program

A program for identifying, recording, collecting, and reporting important resilience information is established and maintained.

Monitoring is not simply a process of accumulating data; instead, it is a process of data collection and distribution with the purpose of providing timely, accurate, complete, and useful information about the current state of operational processes, any potential threats or vulnerabilities, and information about the effectiveness of the organization's operational resilience management activities.

Monitoring encompasses a wide array of organizational activities that serve many different uses and purposes.

For example, monitoring is performed to collect data on

- the secure and accurate functioning of systems and networks
- key performance indicators that demonstrate achievement of strategic objectives and resilience goals

- the actions of persons, objects, and entities when they access and use organizational assets
- vulnerabilities, threats, and risks to organizational assets
- events and incidents that can disrupt organizational assets and services
- the physical movement of persons and objects through organizational facilities and physical plant
- the status of compliance with regulations, laws, and guidelines
- the efficiency of services to meet their goals
- the effectiveness of the organization's internal control system
- activities, issues, and concerns that may require the involvement of organizational oversight or governance
- changes in the organization's risk environment that would warrant changes in operational risk and resilience management strategies
- process efficiency in meeting resilience goals and continually improving

Effective monitoring at an enterprise level is a significant challenge that requires careful planning and program management. Requirements for data collection and distribution must be thoughtfully established by those who need accurate and timely information to manage their processes (commonly referred to as "stakeholders") and to improve them. The extent to which the organization must establish monitoring as an enterprise-level capability depends on the requirements of stakeholders. In many cases, data can be collected efficiently and distributed to many stakeholders, all of which may have vastly different needs for it.

Of note is that not all monitoring activities may be under the direct control of the organization. For example, if the organization has outsourced security operations, many of the monitoring processes relevant to managing operational resilience will probably be performed by the outsourcer and, in some cases, by one of its subcontractors. It is extremely important for the organization to identify where these monitoring processes are being performed and ensure that monitoring requirements (including the accuracy, validity, and timeliness of data) are being met.

To address monitoring as an organizational competency, the organization must establish a monitoring program and plan and identify stakeholders and their requirements as a foundation for an efficient and effective data collection, organization, and distribution process.

MON:SG1.SP1 Establish a Monitoring Program

A program for identifying, collecting, and distributing monitoring information is established and maintained.

The monitoring program establishes the organization's approach to developing, deploying, coordinating, managing, and improving monitoring-related activities (such as data collection and distribution) in order to meet monitoring requirements established by organizational stakeholders. Because monitoring requirements can be vast in scope and breadth, the organization must determine how it can meet these requirements in the most efficient and effective manner.

The monitoring program should address how the organization will perform fundamental monitoring tasks, such as the following:

- identify relevant stakeholders of the monitoring process
- collect monitoring requirements
- analyze and prioritize monitoring requirements based on strategic objectives and business needs
- establish methods, procedures, and processes to collect and distribute data to meet the monitoring requirements
- establish and manage an appropriate infrastructure to support data collection and distribution
- establish and enforce data collection guidelines and standards
- coordinate and manage external entities that have contractual commitments for monitoring processes
- provide guidance on the protection and storage of monitoring data
- perform monitoring

The organization's monitoring program must take into consideration the scope and breadth of the activities necessary to meet these goals, including the human resources necessary to fulfill requirements, the funding required for monitoring processes, and any training or skills improvement activities that will be needed to meet requirements.

Typical work products

1. Monitoring plan and program
2. Documented scope of the monitoring program
3. Documented commitments to the plan and program

Subpractices

1. Establish the plan and scope for a resilience monitoring program.

   In addition to addressing the tasks noted above, the plan and program for monitoring should provide guidance on the types of assets and services that should specifically be included in monitoring activities (i.e., to provide direction on developing monitoring requirements).

2. Establish commitments to the plan.

   Documented commitments by those responsible for implementing and supporting the plan are essential for program effectiveness.

3. Identify internal and external resources (people, tools, sensors, or service providers) that will be used in the monitoring program.
4. Revise the plan and commitments as necessary.

MON:SG1.SP2 Identify Stakeholders

The organizational and external entities that rely upon information collected from the monitoring process are identified.

Stakeholders of the organization's monitoring processes are those internal and external people, entities, or agencies that require information about the operational resilience management processes for which they have responsibility and for which they must achieve resilience goals, objectives, and obligations.

Stakeholders are essential to the monitoring process because their requirements shape and form the monitoring activities that the organization performs. The scope of monitoring is in part devised through the needs of stakeholders of the process, and the tangible processes the organization puts in place to perform monitoring are designed around these needs.

Stakeholders range from high-level personnel such as the CEO and CIO to operations-level staff such as system administrators and security guards.

These are examples of types of stakeholders that may need information from the monitoring process:

- boards of directors and governors
- higher level managers (CXO)
- information technology staff, including
  - system administrators and managers
  - application managers
  - network managers and technicians
  - telecommunications staff
  - security administrators
  - CSIRT teams
- external entities, such as business partners and vendors
- security guards, police, or other public agencies
- external agencies, such as regulatory bodies
- internal and external auditors

The organization must effectively identify stakeholders of the monitoring process and determine their needs and requirements. The identification process may be difficult but can be enabled by reviewing the organization's operational resilience management processes and commencing conversations with stakeholders of these processes. For external stakeholders, the organization may begin with a review of significant contracts with external entities or may have conversations with outsourcers.

The establishment of monitoring requirements is addressed in practice MON:SG1.SP3.

Typical work products

1. List of internal and external stakeholders
2. Stakeholder involvement plan

Subpractices

1. Identify stakeholders of the monitoring process.

The list should include internal and external stakeholders and should be seeded by examining operational resilience management processes and their organizational owners.

2. Develop and document a stakeholder involvement plan.

   To facilitate the organization's enterprise-level monitoring processes, information about the stakeholders and their specific justification for inclusion in the process should be documented.

   These are examples of the type of information that should be collected:

   - rationale for stakeholders' involvement (the processes they own)
   - roles and responsibilities of the relevant stakeholders
   - relationships between stakeholders
   - resources (e.g., training, materials, time, and funding) needed to ensure stakeholder interaction

MON:SG1.SP3 Establish Monitoring Requirements

The requirements for monitoring operational resilience management processes are established.

The scope of the monitoring activity determines how extensive the organization's processes must be and may be a deciding factor in how the organization develops and implements appropriate infrastructure to meet the requirements of stakeholders. The scope is a direct reflection of the needs and requirements of stakeholders.

The requirements of stakeholders must clearly establish the information and data that they need on a regular basis to manage, measure, direct, control, and improve processes for which they have responsibility.

Requirements must consider

- the type and extent of data necessary
- the granularity of data necessary (e.g., by asset, by business process, by service)
- the sources of the data
- who is authorized to distribute, receive, and use the data
- the format(s) of the data (e.g., on paper, electronically, by cell phone, on monitors)
- the distribution frequency of the data and the data refresh (i.e., discretely, such as on a weekly basis, or continuous)
- how the data will be distributed (i.e., remotely, locally)
- the retention of the data (i.e., where it will be stored, by whom, and how it will be protected)
- special needs related to reading, communicating, or understanding the data (systems or special coding books to allow log reading, specialized training, etc.)
- disposition of the data once used

Clearly, these requirements will vary widely by stakeholder and will require extensive consideration and planning to satisfy. In addition, while these requirements form the basis for the organization's program and plan for monitoring, they also establish the requirements for infrastructure that must be implemented and managed to meet the requirements as stated. In some cases, the organization may decide to outsource some of these requirements instead of making permanent investments in infrastructure. *(Infrastructure considerations are addressed in MON:SG2.SP1.)*

The organization must systematically collect, document, analyze, and prioritize the monitoring requirements from stakeholders. However, the organization may also need to decompose these general requirements into functional requirements that relate to resources and infrastructure. For example, if a system administrator needs to have a daily log of the activity of users with special privileges, this log must be able to be produced (by a system or special program) and delivered to the system administrator or the administrator's designees. Thus, the monitoring requirement will have to be translated into other requirements (such as the ability for the operating system to produce the report needed) to be satisfied.

Typical work products

1. Monitoring requirements by stakeholder or process
2. Functional requirements
3. Parameters for requirements refresh and change control

Subpractices

1. Establish monitoring requirements for the operational resilience management processes.

   Monitoring requirements must be established by stakeholder and documented. Essential information about each requirement must be collected so that the requirements can be analyzed and prioritized.

   These are examples of monitoring requirements:

   - audit logs that display the use of trusted user IDs and identities and the actions taken
   - activity logging for the use of application systems
   - control reports that identify violations of or transactions that fail preventive or detective controls
   - logs of changes to access controls
   - logs of entry to and exit from facilities
   - incidents, faults, and alarms
   - maintenance requirements for hardware
   - network traffic monitoring
   - firewall alerts and notifications
   - "whistle-blower" reports of unethical or unacceptable behavior of employees or contractors
   - service desk reports

2. Identify the level and type of monitoring activities required to meet monitoring requirements.

   Monitoring requirements may have to be decomposed to functional requirements in order to determine their feasibility. Functional requirements describe at a detailed level what must be performed to meet the monitoring requirement. At a minimum, functional requirements must specify format, frequency, and source but should also detail infrastructure requirements (if so dependent). If the monitoring requirements will have to be met through a sourcing contract (i.e., via an outsourcer), functional requirements will have to be more extensive so that they can be reflected in requests for proposals (RFPs) and contract terms.

   Examples of functional requirements for a monitoring requirement to "identify violations of preventive and detective controls in a vendor payment system" might include

   - development of a capability to log and store control violations in the vendor payment application
   - real-time, online delivery of alerts to selected managers and supervisors
   - development and distribution of paper-based control reports on a daily basis

3. Establish parameters for requirements refresh and review.

   Because monitoring activities can be labor-, time-, and cost-intensive, monitoring requirements must be reviewed and validated on a regular basis. This allows the organization to avoid monitoring activities that are not purposeful and to direct resources to activities that are next on the priority list.

MON:SG1.SP4 Analyze and Prioritize Monitoring Requirements

Monitoring requirements are analyzed and prioritized to ensure they can be satisfied.

Once requirements have been established for monitoring processes, the organization must determine if the requirements can be satisfied. Satisfaction of the requirements may result in infrastructure and resource needs that the organization does not currently possess and require expenditures for outsourcing or other arrangements to obtain.

Through analysis of monitoring requirements, the organization seeks to determine

- the scope of the requirement (what it covers)
- the potential infrastructure needs to support the requirement
- the resources (human, capital, or expense) needed to support the requirement
- alternatives for meeting the requirement
- requirements that cannot be met, and the potential risk that results
- duplicative requirements or requirements that can be met through efficient data collection (i.e., collect data once, meet many requirements)

The analysis of monitoring requirements is dependent upon a thorough review of functional requirements. Functional requirements express the potential demands on the organization needed to meet monitoring

requirements. If functional requirements cannot be met for any reason (including cost or lack of human resources), alternatives will have to be identified and analyzed (such as outsourcing), or a decision must be made to forgo satisfaction of the requirement.

Because not all monitoring requirements will be able to be met, the organization may need to look at its operational resilience management processes and prioritize requirements so that high-priority needs (such as the detection of events or incidents) are given precedence. Process areas such as Access Management, Vulnerability Analysis and Resolution, Incident Management and Control, Identity Management, and Environmental Control may have significant monitoring needs just to keep them operational and functional.

When the organization cannot meet a requirement, it typically indicates that the information needed to keep operational resilience management processes operating or to improve these processes is not available. In some cases, this may pose additional risk to the organization because events, incidents, vulnerabilities, and threats may go unnoticed or undetected. For example, if the organization is unable to produce a daily log of users who have special privileges and the actions that these users take, there is a potential that unauthorized or inadvertent actions may take place without the organization's knowledge. Thus, not only is the monitoring requirement unfulfilled, but the organization takes on additional risk by not being able to operate a corresponding detective control. This risk must be identified, characterized, and addressed through the organization's risk management process.

Typical work products

1. Prioritized requirements
2. Requirements gaps (or requirements that cannot be met)
3. Alternatives for meeting requirements
4. Risks related to unsatisfied requirements
5. Accepted requirements

Subpractices

1. Analyze monitoring requirements.

   Analysis should address resource and infrastructure needs. Functional requirements should be a primary consideration in analysis because these requirements may become significant constraints in providing monitoring services.

2. Assign priority to monitoring requirements.

   Not all monitoring requirements may be satisfied due to resource constraints. In addition, some requirements may be of higher priority because they support strategies to protect and sustain higher priority assets and services. Thus, the organization should attempt to prioritize monitoring requirements so that qualitative decisions can be made regarding which requirements must be satisfied versus those that may be left unsatisfied.

Requirements on which the organization has put a high priority and which it intends to satisfy should be considered accepted requirements, and appropriate processes should be provided to meet these requirements.

3. Identify monitoring requirements that may not be able to be satisfied.

   Some monitoring requirements may not be able to be satisfied.

   For example, the organization may have

   - resource (human and financial) limitations or constraints
   - lack of adequate infrastructure or supporting processes or technology
   - insufficient funding for outsourcing requirements
   - an inability to determine clear benefits from the investment in satisfying a monitoring requirement

   The organization should clearly document those requirements that cannot be satisfied, communicate this decision to stakeholders (and attempt to negotiate the requirements, if appropriate), and determine any potential consequences that may result.

4. Identify risks that result from unsatisfied requirements.

   In some cases, the inability to satisfy a monitoring requirement may pose additional operational risk to the organization. This is particularly true when monitoring processes are a fundamental part of other operational resilience management processes such as incident management or vulnerability management. In these cases, the inability to satisfy a monitoring requirement should be documented, and any resulting risk should be referred to the organization's risk management process for analysis and resolution.

   The risk management cycle is addressed in the Risk Management process area.

MON:SG2 Perform Monitoring

The monitoring process is performed throughout the enterprise.

Monitoring activities are typically thought of as technology-driven and therefore as part of the domain of information technology. In reality, monitoring activities are often performed throughout the organization, take many forms (from service desk calls to automated monitoring of networks and systems), and involve many different people and their skills.

Effective monitoring requires people, processes, and technology that have to be deployed and managed to meet monitoring requirements and provide timely and accurate information to other operational resilience management processes. This requires the establishment of appropriate infrastructure to support the process, collection standards and processes to ensure consistency and accuracy of information, the active collection of data, and the distribution of data to relevant stakeholders.

Depending on resources, the criticality of the monitoring processes, and the objectives for gathering and distributing monitoring data, the organization may perform monitoring processes, establish infrastructure, and distribute information through internal activities or source some or all of these processes to outsourcers. In some cases, monitoring may be included as part of the outsourcing of an organizational service. Thus, monitoring practices can be performed either in-house or by external entities.

MON:SG2.SP1 Establish and Maintain Monitoring Infrastructure

A monitoring infrastructure commensurate with meeting monitoring requirements is established and maintained.

Monitoring is a data-collection-intensive activity that is often dependent on support services and technologies to meet requirements. While typically a technology-driven activity, many monitoring processes are manual and people-intensive in nature. Relative to the types of monitoring that the organization requires, an appropriate infrastructure must be established and supported to ensure consistent, accurate, and timely satisfaction of requirements. This infrastructure can encompass people, processes, and technology and will likely make use of the organization's existing installed base of technology and manual processes. However, in some cases, the supporting infrastructure may extend beyond the organization's borders to outsourcers and other external entities that help the organization to meet requirements.

Supporting infrastructure may extend beyond the organization's borders where

- the organization does not have a core competency in collecting and distributing required information
- collecting and distributing information are not cost-effective for the organization
- an existing relationship with an external entity can be expanded to meet monitoring requirements

Important considerations for an appropriate supporting infrastructure include the protection and timeliness of data collected and distributed. Monitoring data can expose the organization's weaknesses and therefore must be protected from unauthorized, inappropriate access where it is stored or collected, and in transmission to users and stakeholders. In addition, the timeliness of the collected data is paramount to providing an appropriate response to events, incidents, and threats and other actions the organization may take for improving operational resilience management processes.

In addition to meeting timeliness and protection requirements, the infrastructure should also ensure that the provisions of the organization's monitoring plan and program can be accomplished.

When the infrastructure is not under the direct control of the organization, special contractual arrangements and provisions should be enacted to ensure that protection and timeliness requirements can be met and that corresponding monitoring requirements can be satisfied.

Typical work products

1. Infrastructure requirements
2. Infrastructure map or diagram
3. Data collection tools, techniques, methods, and procedures

Subpractices

1. Identify and inventory existing monitoring infrastructure and capabilities that may address the program objectives and monitoring requirements.

   Monitoring requirements may be able to be met substantially by existing infrastructure and manual processes. Examining existing infrastructure and inventorying existing monitoring capabilities provide the organization an ability to accurately determine additional infrastructure needs and to prepare for meeting them.

2. Identify infrastructure needs to support accepted requirements.

   Infrastructure needs may range from manual processes to automated, highly technical processes and are predicated on monitoring requirements that have been accepted by the organization.

   Based on requirements and existing capabilities, infrastructure requirements have to be articulated and addressed. This process can be aided by examination of the functional requirements that have been developed as a result of analysis of monitoring requirements (as performed in practice MON:SG1.SP3).

   Infrastructure needs that cannot be met by the organization (whether technical or manual) may result in the inability to meet monitoring requirements. In this case, the monitoring requirements that cannot be met, and any resulting risk to the organization, should be characterized and addressed by the organization. *(See subpractice 3 in MON:SG1.SP4.)*

3. Implement and manage monitoring infrastructure.

   An appropriate infrastructure for supporting monitoring requirements must be implemented and managed to ensure consistent and accurate collection and distribution of data.

MON:SG2.SP2 Establish Collection Standards and Guidelines

The standards and parameters for collecting information and managing data are established.

Because monitoring is fundamentally a data collection activity, the organization should implement standards and parameters that ensure enterprise-wide quality assurance for the monitoring process. These standards and parameters should address data accuracy, completeness, and timeliness and should apply across the organization to ensure consistency and repeatability.

Standards and parameters should also address appropriate measures to store monitoring data, to make it available as needed, and to protect it from unacceptable exposure or use. In addition, relevant historical data may be captured as part of the monitoring process that can also provide a foundation for forensic discovery and analysis. This evidence must be appropriately preserved. *(Practices for the appropriate handling of forensic data are specifically addressed in practice IMC:SG2.SP3 in the Incident Management and Control process area.)*

Collection of extraneous or irrelevant information may not instill confidence in stakeholders that the monitoring program is operating as planned or is

meeting the objectives of the program or monitoring requirements. Thus, standards and parameters should also address the filtering and validation of data to ensure it exhibits high levels of integrity.

When collected and stored, monitoring data creates an organizational asset that must be appropriately managed. *(The activities for managing knowledge and information assets are addressed in the Knowledge and Information Management process area.)*

Typical work products

1. Standards and parameters for collection of data
2. Standards and parameters for storage of data
3. Monitoring operating procedures

Subpractices

1. Develop and maintain standards and parameters for collection of monitoring data.

   These are examples of standards and parameters for data collection:
   - defining what needs to be collected based on the monitoring requirements
   - acceptable media for the repository (electronic, paper, etc.)
   - acceptable formats for data
   - validation procedures to ensure data integrity
   - collection time periods, including whether the data collection is discrete or continuous
   - retention period for monitoring data
   - federal, state, or local laws and regulations that may affect how data is collected and stored

2. Develop and maintain standards and parameters for the handling and storage of monitoring data collected.

   These are examples of standards and parameters for storage of data collected:
   - categorizing the information (See KIM:SG1.SP2.)
   - storage and handling procedures for the specific media type (paper or electronic)
   - protection and security standards for monitoring data (by category)
   - retention periods
   - proper procedures for disposal of monitoring data

3. Review, refine, and develop monitoring operating procedures.

   Detailed processes, standard operating procedures, or work instructions may be created during monitoring infrastructure implementation, but they will have to be regularly reviewed, tailored, and possibly supplemented to meet ongoing monitoring needs.

MON:SG2.SP3 Collect and Record Information

Information relevant to the operational resilience management system is collected and recorded.

The basic organizational activities involved in monitoring are data collection and recording. Data collection may be a discrete (i.e., periodic) or continuous activity, depending on the stakeholders' requirements for immediacy, availability, and usability.

Data collection is dependent on having appropriate media to meet the requirements of stakeholders. These requirements may be infrastructure-related (i.e., involve storage arrays, etc.).

Collection media may include

- electronic logs, data files, databases, or information repositories
- paper reports or other physical media such as CDs
- alarms and notifications that warn when a threshold has been reached or exceeded
- real-time surveillance devices, such as video

In a broad sense, monitoring is an activity of not only data collection but also usage of this data to protect and sustain organizational assets and services and to monitor and improve operational resilience management processes. However, the Monitoring process area addresses only the establishment of monitoring requirements and the collection and distribution of relevant monitoring data. It does not address the usage of this data to manage operational resilience or to improve operational resilience processes. The usage of monitoring data is considered to be included as a part of all relevant operational resilience management process areas where appropriate and is not replicated in this process area.

Typical work products

1. Collection methods and procedures
2. Collection media or information repository

Subpractices

1. Develop collection methods and procedures.

   Collection methods and procedures must ensure the organization's ability to meet monitoring requirements (particularly high-priority requirements) with the available infrastructure and capacity.

2. Assign resources to monitoring processes.

   Ensure that monitoring support staff have received appropriate training to perform the necessary monitoring activities.

   These are examples of training:

   - operating, monitoring, and configuring monitoring systems components
   - supporting stakeholders in understanding and interpreting monitoring data
   - securing data collected from monitoring system components

3. Monitor, collect, and record data.
4. Establish and maintain policies for proper handling, labeling, and categorization of data collected during monitoring activities.

These are examples of items to include in policies:

- protection against tampering or unauthorized access
- alterations to the type of data being collected
- log files being edited, deleted, or altered
- storage capacity of collection mechanisms to avoid the file media capacity being exceeded, resulting in overwriting or failing to collect relevant data
- information categorization, labeling, and handling instructions
- requirements for encryption, secure storage, and secure transport or distribution of information

Data categorization is addressed in the Knowledge and Information Management process area.

MON:SG2.SP4 Distribute Information

Collected and recorded information is distributed to appropriate stakeholders.

The continuous and effective management of operational resilience is highly dependent on information collected in the monitoring process.

This information is useful for

- identifying, preventing, and responding to disruptive events
- determining the effectiveness of strategies to protect and sustain assets and services
- determining the effectiveness of operational resilience management processes
- improving operational resilience management processes when necessary

To meet these objectives, monitoring information must be available for use when needed by stakeholders. Thus, the organization must establish viable distribution methods and channels to move collected information to stakeholders as requested in a reliable and consistent manner.

The frequency of distribution of monitoring information is dependent upon the monitoring requirements established by stakeholders. Considering how the monitoring information will be used, stakeholders may require distribution of this information on a discrete basis (i.e., at points in time on a regular basis) or continuously (on demand, highly available). For example, a once-daily report of users who have exercised special privileges may be sufficient for a system security administrator; in contrast, immediate alarms and notifications of potential denial-of-service attacks may be necessary to adequately protect the organization from impact.

The variety and extensiveness of distribution requirements may affect infrastructure capabilities and capacities. Thus, distribution requirements must be included when considering an adequate infrastructure for supporting monitoring processes. *(Considerations of monitoring infrastructure are addressed in practice MON:SG2.SP1.)*

Distribution of monitoring information may also vary significantly depending on whether the monitoring processes are internal or external. External processes may have to be contractually arranged to meet the distribution demands of stakeholders, so their distribution requirements must be clearly identified in contracts and service level agreements.

Typical work products

1. Distribution plans, procedures, and processes
2. Distribution media and methods
3. Distribution channels

Subpractices

1. Identify media and methods of distribution based on requirements.

   Based on requirements for data distribution, the organization should identify the types of media and methods of distribution that will have to be supported to deliver to stakeholders.

   In the case of external collection and distribution of data, the media and methods will have to be included in contractual arrangements and service level agreements.

   Collection media (as described in practice MON:SG2.SP3) may be the same as media used to distribute information. In other words, if data is collected directly to CD it may also be distributed on CD.

   Because monitoring information is a high-value organizational information asset, the protection considerations of this asset must be identified. Appropriate controls may have to be designed and implemented to protect monitoring data from unauthorized use and access. *(Considerations of strategies to protect and sustain information assets are addressed in the Knowledge and Information Management process area.)*

2. Develop and document plans, processes, and procedures for distribution of information to internal and external stakeholders.

   These plans, processes, and procedures should also take into consideration distribution of monitoring information from external sources.

3. Develop infrastructure to meet distribution requirements.

   Monitoring infrastructure is addressed in MON:SG2.SP1.

4. Distribute monitoring information according to requirements.

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 Monitoring process area.

MON:GG1 Achieve Specific Goals

The operational resilience management system supports and enables achievement of the specific goals of the Monitoring process area by

transforming identifiable input work products to produce identifiable output work products.

MON:GG1.GP1 Perform Specific Practices

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

Elaboration:

Specific practices MON:SG1.SP1 through MON:SG2.SP4 are performed to achieve the goals of the monitoring process.

MON:GG2 Institutionalize a Managed Process

Monitoring is institutionalized as a managed process.

MON:GG2.GP1 Establish Process Governance

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

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

Subpractices

1. Establish governance over process activities.

   Elaboration:

   Governance over the monitoring process may be exhibited by

   - developing and publicizing higher level managers' objectives and requirements for the process
   - sponsoring process policies, procedures, standards, and guidelines
   - making higher level managers aware of applicable compliance obligations related to the process, and regularly reporting on the organization's satisfaction of these obligations to higher level managers
   - sponsoring and funding process activities
   - aligning data collection and distribution activities with identified resilience needs and objectives and stakeholder needs and requirements
   - verifying that the process supports strategic resilience objectives
   - 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 prioritizing process requirements and 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 monitoring policy should address

- responsibility, authority, and ownership for performing process activities
- information categorization, labeling, and handling
- protection against tampering and unauthorized access
- encryption, secure storage, and secure transport and distribution of information
- procedures, standards, and guidelines for
  - altering data based on the type of data, including editing, deleting, and altering log files
  - storage capacity of collection mechanisms and actions to take if capacity is exceeded by type of media
  - collection of data
  - recording and storage of data, including collection media (electronic logs, data files, databases, and information repositories)
  - distribution of data, including distribution media, methods, and channels
  - service level agreement terms and conditions for external entities involved in process activities
- methods for measuring adherence to policy, exceptions granted, and policy violations

MON:GG2.GP2 Plan the Process

Establish and maintain the plan for performing the monitoring process.

Elaboration:

The plan for the monitoring process should not be confused with the monitoring plan and program for identifying, collecting, and distributing specific monitoring data as described in specific practice MON:SG1.SP1. The plan for the monitoring process details how the organization will perform monitoring, including the development of specific monitoring plans and programs.

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.

MON:GG2.GP3 Provide Resources

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

Subpractices

1. Staff the process.

Elaboration:

Staff assigned to the monitoring process must have appropriate knowledge of the related processes being monitored and the objectivity to perform monitoring activities without concern for personal detriment and without the expectation of personal benefit.

These are examples of staff required to perform the monitoring process:

- staff responsible for
  - collecting, analyzing, and prioritizing process requirements based on strategic objectives, business needs, and stakeholder requirements and needs
  - developing process plans and programs and ensuring they are aligned with stakeholder requirements and needs
  - establishing an appropriate infrastructure for data collection, recording, and distribution
  - data collection, recording, distribution, and storage
  - data protection and security, so as to ensure data confidentiality, integrity, and availability
  - managing external entities that have contractual obligations for process activities
- owners and custodians of high-value services and assets that support the accomplishment of operational resilience management objectives
- internal and external auditors responsible for reporting to appropriate committees on process effectiveness and the adequacy of collected data to accurately track the performance of operational resilience management processes

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.

Elaboration:

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

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

Elaboration:

Many of these tools, techniques, and methods should be available as applied to other aspects of organizational monitoring. The intent here is to apply these to operational resilience management.

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

- data collection methods, techniques, and tools, including those necessary to manage collection media
- data recording and storage methods, techniques, and tools

- data protection and security methods, techniques, and tools, including those necessary to ensure data confidentiality, integrity, and availability
- data distribution methods, techniques, and tools
- methods, techniques, and tools for developing and managing collection media
- tools for developing and maintaining traceability between stakeholder requirements and process requirements, plans, and programs

MON:GG2.GP4 Assign Responsibility

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

Elaboration:

Specific practice MON:SG1.SP1 calls for documenting commitments by those responsible for implementing the monitoring plan and program. Specific practice MON:SG1.SP2 calls for documenting the roles and responsibilities of relevant stakeholders.

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 monitoring tasks can be formalized by

   - defining roles and responsibilities in the process plan, including roles responsible for collecting, recording, distributing, and ensuring the confidentiality, integrity, and availability of monitoring data
   - including process tasks and responsibility for these tasks in specific job descriptions
   - developing policy requiring organizational unit managers, line of business managers, project managers, and asset and 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.

MON:GG2.GP5 Train People

Train the people performing or supporting the monitoring 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 monitoring process:

   - knowledge of tools, techniques, and methods used to collect, record, distribute, and ensure the confidentiality, integrity, and availability of monitoring data, including those necessary to perform the process using the selected methods, techniques, and tools identified in MON:GG2.GP3 subpractice 3
   - knowledge unique to each type of service, asset, and operational resilience management process area that is required to effectively perform process activities
   - knowledge necessary to elicit and prioritize stakeholder requirements and needs and interpret them to develop effective process requirements, plans, and programs
   - knowledge necessary to analyze and prioritize process requirements
   - knowledge necessary to interpret monitoring data and represent it in ways that are meaningful and appropriate for managers and stakeholders

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:

   - operating, monitoring, and configuring monitoring system components
   - supporting stakeholders in understanding and interpreting monitoring data
   - data collection, recording, distribution, and storage techniques and tools
   - securing data collected from monitoring system components to ensure data confidentiality, integrity, and availability
   - supporting service and asset owners and custodians in understanding the process and their roles and responsibilities with respect to its activities
   - working with external entities that have responsibility for process activities
   - using process methods, tools, and techniques, including those identified in MON:GG2.GP3 subpractice 3

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

MON:GG2.GP6 Control Work Products

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

Elaboration:

These are examples of monitoring work products placed under control:

- process requirements, plans, and programs, including commitments to the plans and programs
- list of internal and external stakeholders and a plan for their involvement
- prioritized process requirements, accepted requirements, and risks resulting from unsatisfied requirements
- infrastructure requirements
- data collection and storage standards and parameters
- data collection, handling, and storage methods, procedures, techniques, and tools
- data distribution plans, procedures, processes, media, methods, and tools
- collection media, including electronic logs, data files, databases, and information repositories
- process plan
- policies and procedures
- contracts with external entities

MON:GG2.GP7 Identify and Involve Relevant Stakeholders

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

Elaboration:

Several MON-specific practices address the involvement of stakeholders in the monitoring process. For example, MON:SG1.SP2 calls for identifying stakeholders that require information about operational resilience management processes for which they are responsible; MON:SG1.SP3 establishes monitoring requirements based on stakeholder requirements and needs.

Subpractices

1. Identify process stakeholders and their appropriate involvement.

   Elaboration:

   These are examples of stakeholders of the monitoring process *(refer to MON:SG1.SP2)*:

   - boards of directors and governors
   - higher level and other managers
   - service owners and asset owners and custodians
   - information technology staff, such as system administrators and CSIRT teams
   - external entities such as business partners, vendors, and outsourcers
   - police and security guards
   - public agencies

- regulatory bodies
- internal and external auditors
- owners of operational resilience management processes
- staff identified as being associated with each process requirement, program, and distribution channel
- staff identified as being associated with each external entity that is collecting and distributing monitoring data

Stakeholders are involved in various tasks in the monitoring process, such as

- establishing requirements for the process
- planning for the process
- establishing process plans and programs
- making decisions about process scope and activities
- assessing collected data
- providing feedback to those responsible for providing the monitoring data on which the analysis results depend
- reviewing and appraising the effectiveness of process activities
- resolving issues in the process

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

MON:GG2.GP8 Measure and Control the Process

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

Elaboration:

Practices in the Monitoring process area provide information about the collection, organization, and distribution of data that can also be applied for measuring and controlling the monitoring process itself.

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 monitoring process:

- percentage of operational resilience management system performance goals for which monitoring data is collected, recorded, and distributed
- percentage of organizational units, services, and activities using monitoring data to assess the performance of operational resilience management processes
- percentage of monitoring requirements accepted (accepted requirements divided by total requirements)
- number of requirements gaps (total requirements minus accepted requirements)
- number of ranked risks resulting from unsatisfied monitoring requirements
- elapsed time from high-value data collection to data distribution to key stakeholders
- number of new, changed, and retired monitoring requirements
- number of times monitoring plan has been revised
- percentage of data collection activities that are automated

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 monitoring process are needed to ensure that

   - the performance of resilience activities is being monitored and regularly reported
   - strategic operational resilience management activities are on track according to plan
   - 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
   - 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.
7. Track corrective action to closure.

MON:GG2.GP9 Objectively Evaluate Adherence

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

Elaboration:

These are examples of activities to be reviewed:

- the alignment of stakeholder requirements and needs with the process scope, requirements, plans, programs, and process plans
- assignment of responsibility, accountability, and authority for resilience process activities
- assignment of responsibility, accountability, and authority for monitoring 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
- verification of monitoring data confidentiality, integrity, and availability controls
- use of monitoring data for improving strategies to protect and sustain assets and services

These are examples of work products to be reviewed:

- process plan and policies
- process scope, requirements, plans, and programs
- data collection, recording, and distribution methods, techniques, and tools
- metrics for the process *(Refer to MON:GG2.GP9 subpractice 2.)*
- contracts with external entities

MON:GG2.GP10 Review Status with Higher Level Managers

Review the activities, status, and results of the monitoring 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.

MON:GG3 Institutionalize a Defined Process

Monitoring is institutionalized as a defined process.

MON:GG3.GP1 Establish a Defined Process

Establish and maintain the description of a defined monitoring 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 monitoring 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.

MON:GG3.GP2 Collect Improvement Information

Collect monitoring 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:

- the degree to which monitoring data is current
- the confidentiality, integrity, and availability status of monitoring data based on integrity and security tests
- metrics and measurements of the viability of the process *(Refer to MON:GG2.GP8 subpractice 2.)*
- changes and trends in operating conditions, risk conditions, and the risk environment that affect process results
- lessons learned in post-event review of incidents and disruptions in continuity
- process lessons learned that can be applied to improve operational resilience management performance
- reports on the effectiveness and weaknesses of controls
- process requirements that are not being satisfied and the risks associated with them
- 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.