Software Engineering Institute

CERT® Resilience Management Model, Version 1.2

Measurement and Analysis (MA)

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/

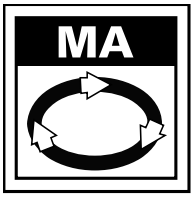
Carnegie Mellon

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

MEASUREMENT AND ANALYSIS

Process



Purpose

The purpose of Measurement and Analysis is to develop and sustain a measurement capability that is used to support management information needs for managing the operational resilience management system.

Introductory Notes

Consistent, timely, and accurate measurements are important feedback for managing any activity. Measurement and Analysis represents a means for applying metrics, measurement, and analysis to the resilience equation. This process area represents the organization's application of measurement as a foundational activity to provide data and analysis results that can be effectively used to inform and improve the management of the resilience process.

In the Measurement and Analysis process area, the organization establishes the objectives for measurement (i.e., what it intends to accomplish) and determines the measures that would be useful to managing the operational resilience management system as well as to providing meaningful data to higher level managers for the processes of governance, compliance, monitoring, and improvement. The organization collects relevant data, analyzes this data, and provides reports to managers and other stakeholders to support decision making.

In a generic sense, the measurement and analysis process includes the following activities and objectives:

- specifying the objectives of measurement and analysis such that they are aligned with identified information needs and objectives
- specifying the measures, analysis techniques, and mechanisms for data collection, data storage, reporting, and feedback
- implementing the collection, storage, analysis, and reporting of the data
- providing objective results that can be used in making informed decisions, and taking appropriate corrective actions

Integrating measurement and analysis into the operational resilience management system supports

- planning, estimating, and executing operational resilience management activities
- tracking the performance of operational resilience management activities against established plans and objectives, including resilience requirements
- identifying and resolving issues in operational resilience management processes
- providing a basis for incorporating measurement into additional operational resilience management processes in the future

Measurement and analysis activities are often most effective when focused at the organizational unit or line of business level. Since operational resilience management is an enterprise-wide concern, however, it's important for the enterprise to have mechanisms in place to make use of that local data at the enterprise level, particularly as the enterprise matures. Repositories for measurement data at the organizational unit or line of business level will be useful for local optimization, but as data is shared across organizational units for the overall improvement benefit of the enterprise, measurement repositories may also be needed at the enterprise level.

Related Process Areas

Measurement and analysis needs are informed by the organization's governance activities, which are addressed in the Enterprise Focus process area.

Some of the data specified for Measurement and Analysis may be gathered and distributed through processes described in the Monitoring process area.

Measurements may be necessary as evidence of compliance; compliance requirements are addressed in the Compliance process area.

Summary of Specific Goals and Practices

Goals	Practices
MA:SG1 Align Measurement and Analysis Activities	MA:SG1.SP1 Establish Measurement Objectives
	MA:SG1.SP2 Specify Measures
	MA:SG1.SP3 Specify Data Collection and Storage Procedures
	MA:SG1.SP4 Specify Analysis Procedures
MA:SG2 Provide Measurement Results	MA:SG2.SP1 Collect Measurement Data
	MA:SG2.SP2 Analyze Measurement Data
	MA:SG2.SP3 Store Data and Results
	MA:SG2.SP4 Communicate Results

Specific Practices by Goal

MA:SG1 Align Measurement and Analysis Activities

Measurement objectives and activities are aligned with identified information needs and objectives.

Measurement activities should provide needed information to the organization's resilience management process and program. Failure to design the measurement and analysis activities in consideration of the organization's needs may lead to inconsistent, incomplete, or inaccurate data collection, inappropriate use or disclosure of measurement data, or inefficient use of measurement resources.

The specific practices covered under this goal may be addressed concurrently or in any order:

- When establishing measurement objectives, experts often think ahead about necessary criteria for specifying measures and analysis procedures. They also think concurrently about the constraints imposed by data collection and storage procedures.

- It often is important to specify the essential analyses that will be conducted before attending to details of measurement specification, data collection, or storage.

MA:SG1.SP1 Establish Measurement Objectives

Measurement objectives are established and maintained based on information needs and objectives.

Measurement objectives document the purposes for which measurement and analysis are done and specify the kinds of actions that may be taken based on the results of data analyses.

The sources for measurement objectives may be management, technical, asset, or process implementation needs.

The measurement objectives may be constrained by existing processes, available resources, or other measurement considerations. Judgments may have to be made about whether the value of the results will be commensurate with the resources devoted to doing the work.

Modifications to identified information needs and objectives may, in turn, be indicated as a consequence of the process and results of measurement and analysis.

Sources of information needs and objectives may be identified at the organizational unit level or at the enterprise level and may include the following:

- monitoring of operational resilience management system performance
- documented management objectives and resilience strategies
- requirements for protecting and sustaining high-value organizational assets and associated services
- risk conditions currently under management consideration
- process improvement objectives and process performance targets
- contractual, legal, and compliance obligations
- supply chain monitoring, including the resilience program status both upstream and downstream
- industry benchmarks
- interviews with managers and other stakeholders that have special information needs

These are examples of measurement objectives:

- Reduce the total number of controls under management.
- Maintain or improve supplier-customer relationships.
- Improve availability or uptime statistics.
- Complete the development (or update) of service continuity plans for the organization.
- Complete risk analyses on all high-value assets and services.
- Regularly test controls and plans to protect and sustain services and assets.
- Improve awareness survey results.
- Improve compliance with regulations, laws, and policies at the lowest cost.

- Provide resilience awareness training to all new employees within three months of hire.
- Complete the implementation or rollout of certain administrative, technical, and physical controls.
- Achieve and improve recovery time objective(s) and/or recovery point objective(s) (RTO and RPO).
- Reduce exposure to known threats and vulnerabilities.
- Improve risk identification.
- Reduce the cost of resilience services and strategies for protecting and sustaining assets.
- Improve the effectiveness and efficiency of measurement and analysis.
- Minimize the total number of access controls under management.
- Achieve internal service level agreements or monitor supplier achievement of external service level agreements.

The development and management of resilience requirements are addressed in the Resilience Requirements Definition and Resilience Requirements Management process areas, respectively. These requirements should be considered in the development of measurement objectives.

(Measurement objectives may overlap with monitoring requirements in that monitoring requirements typically represent information needs that are useful for process control and management. Practice MON:SG1.SP3 focuses on the development of monitoring requirements and should be considered as a source of information for the development of measurement objectives.)

Typical work products

1. Measurement objectives

Subpractices

1. Document information needs and objectives.

   Information needs and objectives are documented to allow traceability to subsequent measurement and analysis activities. *(Refer to MON:SG1.SP3 for information about establishing monitoring requirements that may overlap with measurement information needs and goals.)*

2. Prioritize information needs and objectives.

   It may be neither possible nor desirable to subject all initially identified information needs to measurement and analysis. Priorities may also have to be set within the limits of available resources. *(Refer to MON:SG1.SP4 for information about the prioritization of monitoring requirements.)*

3. Document, review, and update measurement objectives.

   It is important to carefully consider the purposes and intended uses of measurement and analysis.

   The measurement objectives are documented, reviewed by managers and other relevant stakeholders, and updated as necessary. Doing so enables traceability to

subsequent measurement and analysis activities and helps ensure that the analyses will properly address identified information needs and objectives.

It is important that users of measurement and analysis results be involved in setting measurement objectives and deciding on plans of action. It may also be appropriate to involve those who provide the measurement data. *(Refer to MON:SG1.SP2 for information about the establishment of monitoring stakeholders and their inclusion in the monitoring process. These stakeholders may also provide information to, or receive information from, the measurement and analysis process.)*

4. Provide feedback for refining and clarifying information needs and objectives as necessary.

   Identified information needs and objectives may have to be refined and clarified as a result of setting measurement objectives. Initial descriptions of information needs may be unclear or ambiguous. Conflicts may arise between existing needs and objectives. Precise targets on an already existing measure may be unrealistic.

5. Maintain traceability of the measurement objectives to the identified information needs and objectives.

   There must always be a good explanation for why a measurement is being analyzed.

   Of course, the measurement objectives may also change to reflect evolving information needs and objectives.

MA:SG1.SP2 Specify Measures

The measures necessary to meet measurement objectives are established.

Measurement objectives are refined into precise, quantifiable measures.

Measures may be either "base" or "derived." Data for base measures is obtained by direct measurement. Data for derived measures comes from other data, typically by combining two or more base measures.

These are examples of base measures:

- number of high-value assets by category (people, information, technology, facilities)
- number of risk analyses conducted during a certain period of time
- number of vulnerabilities identified in a specific time range
- total number of controls under management
- number of service continuity plans updated within the past 12 months
- total number of incidents declared in the past quarter

These are examples of derived measures:

- percentage of high-value technology assets for which a risk analysis was conducted in the previous 12 months
- percentage of staff who have undergone resilience policy training in the previous 12 months
- percentage of vulnerabilities identified in the past month that have been analyzed and resolved
- trends (growth or decline) in incidents declared

- trends in time elapsed from incident declaration to closure
- percentage of unmet test objectives for exercising service continuity plans
- percentage of vital staff (or resilience staff) who have participated in service continuity plan exercises in the past year

Derived measures typically are expressed as ratios, composite indices, or other aggregate summary measures. They are often more quantitatively reliable and meaningfully interpretable than the base measures used to generate them.

Typical work products

1. Specifications of base and derived measures

Subpractices

1. Identify candidate measures based on documented measurement objectives.

   The measurement objectives are refined into specific measures. The identified candidate measures are categorized and specified by name and unit of measure.

2. Identify existing measures that already address the measurement objectives.

   Specifications for measures may already exist, perhaps established for other purposes earlier or elsewhere in the organization.

3. Specify operational definitions for the measures.

   Operational definitions are stated in precise and unambiguous terms. They address two important criteria:

   - Communication—What has been measured, how was it measured, what are the units of measure, and what has been included or excluded?
   - Repeatability—Can the measurement be repeated, given the same definition, to get the same results?

4. Prioritize, review, and update measures.

   Proposed specifications of the measures are reviewed for their appropriateness with potential end users and other relevant stakeholders. Priorities are set or changed, and specifications of the measures are updated as necessary.

MA:SG1.SP3 Specify Data Collection and Storage Procedures

The techniques for collecting and storing measurement data are specified.

Explicit specification of collection methods helps ensure that the right data is collected properly. It may also aid in further clarifying information needs and measurement objectives.

Proper attention to storage and retrieval procedures helps ensure that data is available and accessible for future use and that the information is adequately protected and sustained according to applicable resilience requirements.

(Monitoring activities, particularly for the collection, storage, and distribution of data, may overlap significantly with MA:SG1.SP3. Specifically, MON:SG2.SP1, Establish and Maintain Monitoring Infrastructure, MON:SG2.SP3, Collect and Record Information, and MON:SG2.SP4, Distribute Information, may all be useful for achieving MA:SG1.SP3 if the information being monitored for and collected is related directly to measurement and analysis activities.)

Typical work products

1. Data collection and storage procedures
2. Data collection tools

Subpractices

1. Identify existing sources of data that is generated from current processes or transactions.

   Existing sources of data may already have been identified when specifying the measures. Appropriate collection mechanisms may exist whether or not pertinent data has already been collected.

2. Identify measures for which data is needed but is not currently available.
3. Specify how to collect and store the data for each required measure.

   Explicit specifications are made for how, where, and when the data will be collected. Procedures for collecting valid data are specified. The data is stored in an accessible manner for analysis, and it is determined whether it will be saved for possible re-analysis or documentation purposes.

   Questions to be considered typically include the following:

   - Have the frequency of collection and the points in the process where measurements will be made been determined?
   - Has the timeline that is required to move measurement results from the points of collection to repositories, other databases, or end users been established?
   - Who is responsible for obtaining the data?
   - Who is responsible for data storage, retrieval, and security?
   - Have necessary supporting tools been developed or acquired?
   - What are the resilience requirements for the data?

   Practice MON:SG2.SP2 establishes information collection standards and parameters that may be useful for collecting measurement and analysis data. If measurement and analysis data is collected through a monitoring process, the collection specifications should be included in the standards and parameters.

4. Create data collection mechanisms and process guidance.

   Data collection and storage mechanisms are well integrated with other normal work processes. Data collection mechanisms may include manual or automated forms and templates. Clear, concise guidance on correct procedures is available to those responsible for doing the work. Training is provided as necessary to clarify the processes necessary for collection of complete and accurate data and to minimize the burden on those who must provide and record the data.

5. Support automatic collection of the data where appropriate and feasible.

   Automated support can aid in collecting more complete and accurate data.

   These are examples of such automated support:

   - asset counts from inventory management systems
   - employee population from human resources management systems
   - automated tracking of system availability statistics
   - automatic counts and statistics from event or incident tracking systems
   - statistics from automated patch and configuration management tools

   However, some data cannot be collected without human intervention (e.g., customer satisfaction or other human judgments), and setting up the necessary infrastructure for other automation may be costly.

   Practice MON:SG1.SP2 addresses the essential infrastructure necessary to meet data collection, storage, and distribution standards for monitoring purposes. This infrastructure and the related infrastructure requirements may overlap those of the measurement and analysis process.

6. Prioritize, review, and update data collection and storage procedures.

   Proposed procedures are reviewed for their appropriateness and feasibility with those who are responsible for providing, collecting, and storing the data. They also may have useful insights about how to improve existing processes or may be able to suggest other useful measures or analyses. *(See MON:SG2.SP2 for related activities.)*

7. Update measures and measurement objectives as necessary.

   Priorities may have to be reset based on the following:

   - the importance of the measures
   - the amount of effort required to obtain the data

   Considerations include whether new forms, tools, or training would be required to obtain the data.

MA:SG1.SP4 Specify Analysis Procedures

The techniques for analysis and reporting are specified.

Specifying the analysis procedures in advance ensures that appropriate analyses will be conducted and reported to address the documented measurement objectives (and thereby the information needs and objectives on which they are based). This approach also provides a check that the necessary data will in fact be collected.

For operational resilience management purposes, analysis methods and techniques are likely to be extensive and cover a wide range of disciplines.

Typical work products

1. Analysis specifications and procedures
2. Data analysis tools

Subpractices

1. Specify and prioritize the analyses that will be conducted and the reports that will be prepared.

   Early attention should be paid to the analyses that will be conducted and to the manner in which the results will be reported. These should meet the following criteria:

   - The analyses explicitly address the documented measurement objectives.
   - Presentation of the results is clearly understandable by the audiences to whom the results are addressed.

   Priorities may have to be set within available resources.

2. Select appropriate data analysis methods and tools.

   Issues to be considered typically include the following:

   - choice of visual display and other presentation techniques (e.g., pie charts, bar charts, histograms, radar charts, line graphs, scatter plots, or tables)
   - choice of appropriate descriptive statistics (e.g., arithmetic mean, median, or mode)
   - decisions about statistical sampling criteria when it is impossible or unnecessary to examine every data element
   - decisions about how to handle analysis in the presence of missing data elements
   - selection of appropriate analysis tools

   Descriptive statistics are typically used in data analysis to do the following:

   - examine distributions on the specified measures (e.g., central tendency, extent of variation, or data points exhibiting unusual variation)
   - examine the interrelationships among the specified measures (e.g., comparisons of incident types and frequency across organizational units or lines of business)
   - display changes over time

3. Specify administrative procedures for analyzing the data and communicating the results.

   Issues to be considered typically include the following:

   - identifying the persons and groups responsible for analyzing the data and presenting the results
   - determining the timeline to analyze the data and present the results
   - determining the venues for communicating the results (e.g., progress reports, transmittal memos, written reports, or staff meetings)

4. Review and update the proposed content and format of the specified analyses and reports.

   All of the proposed content and format are subject to review and revision, including analytic methods and tools, administrative procedures, and priorities. The relevant stakeholders consulted should include intended end users, sponsors, data analysts, and data providers.

5. Update measures and measurement objectives as necessary.

   Just as measurement needs drive data analysis, clarification of analysis criteria can affect measurement. Specifications for some measures may be refined further based

on the specifications established for data analysis procedures. Other measures may prove to be unnecessary, or a need for additional measures may be recognized.

The exercise of specifying how measures will be analyzed and reported may also suggest the need for refining the measurement objectives themselves.

6. Specify criteria for evaluating the utility of the analysis results and for evaluating the conduct of the measurement and analysis activities.

Criteria for evaluating the utility of the analysis might address the extent to which the following apply:

- The results are (1) provided on a timely basis, (2) understandable, and (3) used for decision making.
- The work does not cost more to perform than is justified by the benefits that it provides.

Criteria for evaluating the conduct of the measurement and analysis might include the extent to which the following apply:

- The amount of missing data or the number of flagged inconsistencies is beyond specified thresholds.
- There is selection bias in sampling (e.g., only satisfied end users are surveyed to evaluate end-user satisfaction, or only unsuccessful projects are evaluated to determine overall productivity).
- The measurement data are repeatable (e.g., statistically reliable).
- Statistical assumptions have been satisfied (e.g., about the distribution of data or about appropriate measurement scales).

MA:SG2 Provide Measurement Results

Measurement results, which address identified information needs and objectives, are provided.

The primary reason for performing measurement and analysis is to address identified information needs and objectives. Measurement results based on objective evidence can help to monitor performance, achieve resilience plan obligations, fulfill compliance obligations, make informed management and technical decisions, and enable corrective actions to be taken.

MA:SG2.SP1 Collect Measurement Data

Measurement data is collected consistent with measurement objectives.

The data necessary for analysis is obtained and checked for completeness and integrity.

Practice MON:SG2.SP3 specifically addresses the collection of monitoring data that may also include measurement data for the purposes of measurement and analysis.

Typical work products

1. Base and derived measurement data sets
2. Results of data integrity tests

Subpractices

1. Obtain the data for base measures.

   Data is collected as necessary for previously used as well as for newly specified base measures.

   Data that was collected earlier may no longer be available for reuse in existing databases, paper records, or formal repositories.

2. Generate the data for derived measures.

   Values are newly calculated for all derived measures.

3. Perform data integrity checks as close to the source of the data as possible.

   All measurements are subject to error in specifying or recording data. It is always better to identify such errors and to identify sources of missing data early in the measurement and analysis cycle.

   Checks can include scans for missing data, out-of-bounds data values, and unusual patterns and correlation across measures. It is particularly important to do the following:

   - Test and correct for inconsistency of categorizations made by human judgment (i.e., to determine how frequently people make differing categorization decisions based on the same information, otherwise known as "inter-coder reliability").
   - Empirically examine the relationships among the measures that are used to calculate additional derived measures. Doing so can ensure that important distinctions are not overlooked and that the derived measures convey their intended meanings (otherwise known as "criterion validity").

   Controls over information that are relevant to measurement and analysis are addressed in KIM:SG5.SP3 in the Knowledge and Information Management process area.

MA:SG2.SP2 Analyze Measurement Data

Measurement data is analyzed against measurement objectives.

The measurement data is analyzed as planned, additional analyses are conducted as necessary, results are reviewed with relevant stakeholders, and necessary revisions for future analyses are noted.

Typical work products

1. Analysis results and draft reports

Subpractices

1. Conduct initial analyses, interpret the results, and draw preliminary conclusions.

   The results of data analyses are rarely self-evident. Criteria for interpreting the results and drawing conclusions should be stated explicitly.

2. Conduct additional measurement and analysis as necessary, and prepare results for presentation.

The results of planned analyses may suggest (or require) additional, unanticipated analyses. In addition, they may identify needs to refine existing measures, to calculate additional derived measures, or even to collect data for additional base measures to properly complete the planned analysis. Similarly, preparing the initial results for presentation may identify the need for additional, unanticipated analyses.

3. Review the initial results with relevant stakeholders.

   It may be appropriate to review initial interpretations of the results and the way in which they are presented before distributing and communicating them more widely.

   Reviewing the initial results before their release may prevent needless misunderstandings and lead to improvements in the data analysis and presentation.

   Relevant stakeholders with whom reviews may be conducted include asset owners and custodians, resilience staff, vital management personnel, and data providers.

4. Refine criteria for future analyses.

   Valuable lessons that can improve future efforts are often learned from conducting data analyses and preparing results. Similarly, ways to improve measurement specifications and data collection procedures may become apparent, as may ideas for refining identified information needs and objectives.

MA:SG2.SP3 Store Data and Results

Measurement data, analyses, and results are stored.

Storing measurement-related information enables the timely and cost-effective future use of historical data and results. The information also is needed to provide sufficient context for interpretation of the data, measurement criteria, and analysis results.

Information stored typically includes the following:

- measurement plans
- specifications of measures
- sets of data that have been collected
- analysis reports and presentations

The stored information contains or references the information needed to understand and interpret the measures and to assess them for reasonableness and applicability (e.g., measurement specifications used in different business units when comparing across business units).

Data sets for derived measures typically can be recalculated and need not be stored. However, it may be appropriate to store summaries based on derived measures (e.g., charts, tables of results, or report prose).

Interim analysis results need not be stored separately if they can be efficiently reconstructed.

The organization should determine whether to store data in a centralized manner at the enterprise level, in a decentralized manner at the organizational unit level, or some combination.

Measurement and analysis data may constitute an organizational asset that requires controls to ensure confidentiality, integrity, and availability. *(Controls over information assets are addressed in the Knowledge and Information Management process area.)*

Typical work products

1. Stored data inventory

Subpractices

1. Review the data to ensure its completeness, integrity, accuracy, and currency.
2. Store the data according to the data storage procedures.
3. Make the stored contents available for use only by appropriate groups and staff.
4. Prevent the stored information from being used inappropriately.

   Ways to prevent inappropriate use of the data and related information include controlling access to data and educating people on the appropriate use of information.

   These are examples of inappropriate use:

   - disclosure of information that was provided in confidence
   - faulty interpretations based on incomplete, out-of-context, or otherwise misleading information
   - measures used to improperly evaluate the performance of people
   - impugning the integrity of specific individuals

   Specific controls over the confidentiality, integrity, and availability of measurement information are specified in goal KIM:SG4 in the Knowledge and Information Management process area.

MA:SG2.SP4 Communicate Results

The results of measurement and analysis activities are communicated to relevant stakeholders.

The results of the measurement and analysis process are communicated to relevant stakeholders in a timely and usable fashion to support decision making and assist in taking corrective action.

Relevant stakeholders include risk managers and higher level managers, relevant resilience staff, asset owners and custodians, data analysts, and data providers.

Typical work products

1. Delivered reports and related analysis results
2. Contextual information or guidance to aid in the interpretation of analysis results

Subpractices

1. Keep relevant stakeholders apprised of measurement results on a timely basis.

Measurement results are communicated in time to be used for their intended purposes. Reports are unlikely to be used if they are distributed with little effort to follow up with those who need to know the results.

To the extent possible and as part of the normal way they do business, users of measurement results are kept personally involved in setting objectives and deciding on plans of action for measurement and analysis. The users are regularly kept apprised of progress and interim results.

2. Assist relevant stakeholders in understanding the results.

Results are reported in a clear and concise manner appropriate to the methodological sophistication of the relevant stakeholders. They are understandable, easily interpretable, and clearly tied to identified information needs and objectives.

The data is often not self-evident to practitioners who are not measurement experts. Measurement choices should be explicitly clear about the following:

- how and why the base and derived measures were specified
- how the data was obtained
- how to interpret the results based on the data analysis methods that were used
- how the results address information needs

These are examples of actions to assist in the understanding of results:

- discussing the results with the relevant stakeholders
- providing a transmittal memo that provides background and explanation
- briefing users on the results
- providing training on the appropriate use and understanding of measurement results

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 Measurement and Analysis process area.

MA:GG1 Achieve Specific Goals

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

MA:GG1.GP1 Perform Specific Practices

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

Elaboration:

Specific practices MA:SG1.SP1 through MA:SG2.SP4 are performed to achieve the goals of the measurement and analysis process.

MA:GG2 Institutionalize a Managed Process

Measurement and analysis is institutionalized as a managed process.

MA:GG2.GP1 Establish Process Governance

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

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

Subpractices

1. Establish governance over process activities.

   Elaboration:

   Governance over the measurement and analysis process may be exhibited by

   - developing and publicizing higher level managers' objectives for the process
   - sponsoring process policies, procedures, standards, and guidelines
   - sponsoring and funding process activities
   - aligning measurement data collection and analysis 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 improving the process
   - providing input on identifying, assessing, and managing operational risks to high-value services and assets
   - 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 measurement and analysis policy should address

   - responsibility, authority, and ownership for performing process activities
   - procedures, standards, and guidelines for
     - specifying measures based on measurement objectives
     - analyses of measurement data
     - collection of measurement data
     - storage of measurement data
     - reporting of measurement data
     - establishing measurement repositories
   - methods for measuring adherence to policy, exceptions granted, and policy violations

MA:GG2.GP2 Plan the Process

Establish and maintain the plan for performing the measurement and analysis process.

Elaboration:

The plan for the measurement and analysis process should not be confused with measurement plans for collecting, analyzing, storing, and communicating specific measurement data as described in specific goal MA:SG2. The plan for the measurement and analysis process details how the organization will perform measurement and analysis, including the development of specific measurement plans.

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.

MA:GG2.GP3 Provide Resources

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

Subpractices

1. Staff the process.

   Elaboration:

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

   These are examples of staff required to perform the measurement and analysis process:

   - staff responsible for
     - specifying process objectives and ensuring they are aligned with information needs and objectives
     - specifying measures, analysis techniques, and mechanisms for data collection, storage, reporting, and feedback
     - data collection, storage, analysis, and reporting
     - providing results to inform decision making and developing plans of action
     - developing measurement plans and programs and ensuring they are aligned with stakeholder requirements and needs
     - managing external entities that have contractual obligations for measurement and analysis 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 measures 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.

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

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 measurement and analysis. The intent here is to apply these to operational resilience management.

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

- statistical software tools
- data collection, storage, and analysis methods, techniques, and tools, including those necessary to ensure data integrity and security
- tools to assist in calculating derived measures from base measures
- data reporting methods, techniques, and tools, including techniques for visual display and presentation of data
- techniques to assist in interpreting results based on the data analysis methods that were used
- methods, techniques, and tools for developing and managing measurement inventories, databases, and repositories
- tools for developing and maintaining traceability between information needs and measurement objectives

MA:GG2.GP4 Assign Responsibility

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

Elaboration:

Specific practice MA:SG1.SP3 calls for determining responsibilities for data collection, storage, retrieval, and security. Specific practice MA:SG1.SP4 calls for identifying those responsible for data analysis and presentation.

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 measurement and analysis tasks can be formalized by

   - defining roles and responsibilities in the process plan to include roles responsible for providing, collecting, analyzing, storing, retrieving, reporting, and ensuring the integrity and security of measurement 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 tasks 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.

MA:GG2.GP5 Train People

Train the people performing or supporting the measurement and analysis 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 measurement and analysis process:

   - knowledge of tools, techniques, and methods used to collect, analyze, store, retrieve, report, and ensure the integrity and security of measurement data,

including those necessary to perform the process using the selected methods, techniques, and tools identified in MA:GG2.GP3 subpractice 3

- knowledge unique to each type of service and asset that is required to effectively perform process activities
- knowledge necessary to elicit and prioritize information needs and objectives and interpret them to develop effective measurement objectives
- knowledge necessary to identify measurement specifications that reflect measurement objectives
- knowledge necessary to interpret measurement data and represent it in reports 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:

- statistical or other analysis techniques
- data collection, analysis, and reporting techniques
- data storage techniques
- development of resilience measurements that reflect information needs and objectives
- supporting service and asset owners and custodians in understanding the process and their roles and responsibilities with respect to its activities
- using process methods, tools, and techniques, including those identified in MA:GG2.GP3 subpractice 3

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

MA:GG2.GP6 Control Work Products

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

Elaboration:

These are examples of measurement and analysis work products placed under control:

- measurement objectives
- measurement specifications
- data collection and storage procedures and tools
- data analysis specifications, procedures, and tools
- measurement data sets
- analysis results, reports, and presentations
- data inventories, repositories, and databases
- process plan
- policies and procedures
- contracts with external entities

MA:GG2.GP7 Identify and Involve Relevant Stakeholders

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

Elaboration:

Several MA-specific practices address the involvement of stakeholders in the measurement and analysis process. For example, MA:SG1.SP1 calls for involving relevant stakeholders in the formulation of measurement objectives, and MA:SG1.SP2 calls for involving them in the prioritization and review of measurement specifications.

Subpractices

1. Identify process stakeholders and their appropriate involvement.

   Elaboration:

   These are examples of stakeholders of the measurement and analysis process:

   - service owners and asset owners and custodians
   - staff involved in specifying and prioritizing information needs
   - staff involved in establishing measurement objectives, measures, procedures, and techniques
   - staff involved in prioritizing, reviewing, and updating specifications of measures
   - end users, sponsors, data analysts, and data providers involved in reviewing and updating proposed content and format of specified analyses and reports
   - staff involved in assessing and interpreting measurement data and deciding on plans of action (Early reviewers of analysis results may include asset owners and custodians, resilience staff, vital management personnel, and data providers. Decision makers include risk managers and higher level managers, relevant resilience staff, asset owners and custodians, data analysts, and data providers.)
   - users of measurement results, including organizational unit and line of business managers
   - staff involved in providing meaningful feedback to those responsible for providing the raw data on which measurement analysis and results depend
   - external entities responsible for managing high-value services, assets, and outsourced functions
   - internal and external auditors

   Stakeholders are involved in various tasks in the measurement and analysis process, such as

   - establishing requirements for the process
   - planning for the process
   - establishing measurement objectives and plans
   - making decisions about process activities
   - assessing measurement data, results, and reports
   - providing feedback to those responsible for providing the raw 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.

MA:GG2.GP8 Measure and Control the Process

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

Elaboration:

While this practice is self-referencing, practices in the Measurement and Analysis process area provide information about measuring and analyzing operational resilience management processes that can also be applied to the measurement and analysis process.

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 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 measurement and analysis process:
   - percentage of measurement objectives that can be traced to information needs and objectives
   - percentage of measures for which operational definitions have been specified
   - percentage of measurement objectives achieved (against defined targets, if relevant)
   - percentage of operational resilience management system performance goals for which measurement data is collected, analyzed, and communicated
   - percentage of organizational units, services, and activities using operational resilience management measures to assess the performance of operational resilience management processes
   - elapsed time between collection, analysis, and communication of measurement data
   - percentage of measures that can be traced to measurement objectives
   - percentage of measures whose collection, analysis, and reporting is automated
   - percentage of specified measures that are collected, analyzed, and stored
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 measurement and analysis process are needed to ensure that

- the performance of resilience activities is being measured 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 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.

MA:GG2.GP9 Objectively Evaluate Adherence

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

Elaboration:

These are examples of activities to be reviewed:

- the alignment of information needs and objectives with measurement objectives; the alignment of measurement objectives with measurement specifications
- the alignment of stakeholder requirements with process plans
- assignment of responsibility, accountability, and authority for resilience process activities
- assignment of responsibility, accountability, and authority for measurement and analysis activities
- determining the adequacy of measurement 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 measurement data integrity and security controls
- use of measurement data for improving strategies to protect and sustain assets and services

These are examples of work products to be reviewed:

- process plan and policies
- measurement objectives
- specifications for base and derived measures
- data collection, analysis, and storage methods, techniques, and tools
- analysis results, reports, and presentations, including variance from required performance indicators and targets and trends in base and derived measures
- metrics for the process *(Refer to MA:GG2.GP9 subpractice 2.)*

MA:GG2.GP10 Review Status with Higher Level Managers

Review the activities, status, and results of the measurement and analysis 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.

MA:GG3 Institutionalize a Defined Process

Measurement and analysis is institutionalized as a defined process.

MA:GG3.GP1 Establish a Defined Process

Establish and maintain the description of a defined measurement and analysis 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 measurement and analysis 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.

MA:GG3.GP2 Collect Improvement Information

Collect measurement and analysis work products 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 measurement data is current
- the integrity and security status of measurement data based on integrity and security tests
- data analysis reports and presentations
- changes and trends in operating conditions, risk conditions, and the risk environment that affect measurement 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.