Software Engineering Institute

CERT® Resilience Management Model, Version 1.2

Glossary of Terms

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

GLOSSARY OF TERMS

This document contains an alphabetical glossary of terms for the CERT Resilience Management Model. The glossary provides definitions based on how the term is used in the context of operational resilience management. For this reason, the definitions provided may differ from those in common use.

For terms that relate directly to a process area, the process area acronym is noted in brackets at the end of each definition. For example, [AM] refers to the Access Management process area.

Abuse case
See *misuse/abuse case*.

Access acknowledgment
A form or process that allows users to acknowledge (in writing) that they understand their access privileges and will abide by the organization's policy regarding the assignment, use, and revocation of those privileges. [AM]

Access control
The administrative, technical, or physical mechanism that provides a "gate" at which identities must present proper credentials and be authenticated to pass. [AM] [KIM]

Access control policy (access management policy)
An organizational policy that establishes the policies and procedures for requesting, approving, and providing access to persons, objects, and entities and establishes the guidelines for disciplinary action for violations of the policy. [AM]

Access Management (AM)
An operations process area in CERT-RMM. The purpose of Access Management is to ensure that access granted to organizational assets is commensurate with their business and resilience requirements.

Access privilege
A mechanism for describing and defining an appropriate level of access to an organizational asset—information, technology, or facilities—commensurate with an identity's job responsibilities and the business and resilience requirements of the asset. [AM] [HRM]

Access request
A mechanism for requesting access to an organizational asset that is submitted to and approved by owners of the asset (with sufficient justification). [AM]

Acculturation
The acquisition and adoption of a process improvement mind-set and culture for resilience throughout all levels of the organization. [HRM]

Adaptive maintenance
Maintenance performed to adapt a facility to a different operating environment. [EC]

Administrative control
A type of managerial control that ensures alignment to management's intentions. It includes such artifacts as governance, policy, monitoring, auditing, separation of duties, and the development and implementation of service continuity plans. [KIM]

Agreement
A legal agreement between the organization and a business partner or supplier. The agreement may be a contract, a license, or a memorandum of agreement (MOA). The agreement is legally binding. Performance measures against the agreement are typically created and documented in a service level agreement (SLA), a secondary agreement that often supports the legal agreement.

Appraisal scope
The part of the organization that is the focus of a CERT-RMM-based appraisal of current resilience practices. The scope of an appraisal is typically, but not necessarily, the same as the scope of the improvement effort. (See the related terms *model scope* and *organizational scope*.)

Asset (organizational asset)
Something of value to the organization, typically, people, information, technology, and facilities that high-value services rely on. [ADM]

Asset custodian
A person or organizational unit, internal or external to the organization, responsible for satisfying the resilience requirements of a high-value asset while it is in its care. For example, a system administrator on a server that contains the vendor database would be a custodian of that asset. [ADM] [RRM]

Asset Definition and Management (ADM)
An engineering process area in CERT-RMM. The purpose of Asset Definition and Management is to identify, document, and manage organizational assets during their life cycle to ensure sustained productivity to support organizational services.

Asset disposition
The retirement of an asset from service, particularly an information asset, commensurate with resilience requirements and information categorization and in accordance with any applicable rules, laws, and regulations. [KIM]

Asset inventory
An inventory (or inventories) of organizational assets—people, information, technology, and facilities. [ADM]

Asset-level resilience requirements
Asset-specific requirements that are set by the owners of an asset. They are intended to establish the asset's protection and sustainment needs with respect to its role in supporting mission assurance of a high-value service. [RRD]

Asset life cycle
The phases of an asset's life from development or acquisition to deployment to disposition. [ADM]

Asset owner
A person or organizational unit (internal or external to the organization) with primary responsibility for the viability, productivity, and resilience of an organizational asset. For example, the accounts payable department is the owner of the vendor database. [ADM] [RRM]

Asset profile
Documentation of specific information about an asset (typically an information asset) that establishes ownership, a common definition, and other characteristics of the asset, such as its value. [ADM]

Assurance case
A structured set of arguments and a corresponding body of evidence demonstrating that a system satisfies specific claims with respect to its security, safety, or reliability properties. [RTSE]

Attack pattern
A design pattern describing the techniques that attackers might use to break a software product. [RTSE]

Attack surface
The set of ways in which an attacker can enter and potentially cause damage to a system. The larger the attack surface, the more insecure the system [Manadhata 2010]. [RTSE]

Availability
For an asset, the quality of being accessible to authorized users (people, processes, or devices) whenever it is needed. [EC] [KIM] [PM]

Awareness
Focusing the attention of, creating cognizance in, and acculturating people throughout the organization to resilience issues, concerns, policies, plans, and practices. [OTA]

Awareness activity
A means for implementing the awareness approaches that the organization has considered and developed to meet the specific needs of the stakeholder community. Formal awareness training sessions, newsletters, email messages, and posters and other signage are examples of awareness activities. [OTA]

Awareness training
A means by which the organization can highlight important behaviors and begin the process of acculturating staff and business partners to important organizational resilience goals, objectives, and critical success factors. [OTA]

Awareness training waiver
See *waiver*.

Base measures
Data obtained by direct measurement (for example, the number of service continuity plans updated in the last 12 months). [MA]

Baseline configuration item
A configuration item that serves as the baseline foundation for managing the integrity of an asset as it changes over its life cycle. [TM]

Business process
A series of discrete activities or tasks that contribute to the fulfillment of a service mission. (See the related term *service*.)

Business requirement
A requirement that must be met to achieve business objectives. Such requirements establish the baseline for how organizational assets are used to support business processes. [ADM]

Capability level
An indicator of achievement of process capability in a process area. A capability level is achieved by visibly and verifiably implementing the required components of a process area. (See the related terms *required component* and *process area*.)

Capacity planning
The process of determining the operational demand for a technology asset over a widely variable range of operational needs. [TM]

Change control (change management)
A continuous process of controlling changes to information or technology assets, related infrastructure, or any aspect of services, enabling approved changes with minimum disruption. [KIM] [RRM] [TM]

Co-location (also collocation or colocation)
The act or result of placing or arranging together. In facilities management, co-location refers to the grouping of facilities, the effects of which must be considered in service continuity planning. [EC]

Communications (COMM)
An enterprise process area in CERT-RMM. The purpose of Communications is to develop, deploy, and manage internal and external communications to support resilience activities and processes.

Communications stakeholder
A person or group with a vested interest in being involved in or a beneficiary of the organization’s resilience communications activities. [COMM]

Compliance (COMP)
An enterprise process area in CERT-RMM. The purpose of Compliance is to ensure awareness of and compliance with an established set of relevant internal and external guidelines, standards, practices, policies, regulations, and legislation, and other obligations (such as contracts and service level agreements) related to managing operational resilience.

Compliance
A process that characterizes the activities that the organization performs to identify the internal and external guidelines, standards, practices, policies, regulations, and legislation to which they are subject and to comply with these obligations in an orderly, systematic, efficient, timely, and accurate manner. [COMP]

Compliance knowledgebase
A common accessible information repository for compliance data. The repository may include documentation of the compliance obligations and their owners and due dates, the results of compliance and substantive testing of controls, compliance targets and metrics, compliance reports, non-compliance reports, remediation plans, and tracking data to provide status on satisfying compliance obligations. [COMP]

Compliance obligations
The internal and external guidelines, standards, practices, policies, regulations, and legislation with which the organization has an obligation to comply. [COMP]

Condition
A term that collectively describes a vulnerability, an actor, a motive, and an undesirable outcome. A condition is essentially a threat that the organization must identify and analyze to determine if exploitation of the threat could result in undesirable consequences. [RISK] (See the related term *consequence*.)

Confidentiality
For an asset, the quality of being accessible only to authorized people, processes, and devices. [KIM]

Configuration item
An asset or a series of related assets (typically information- or technology-focused) that are placed under configuration management processes. [KIM] [TM]

Configuration management
A process for managing the integrity of an information or technology asset over its lifetime. Typically includes change control processes. [KIM] [TM]

Consequence
The unwanted effect, undesirable outcome, or impact on the organization that results from the exploitation of a condition or threat. [RISK] (See the related term *condition*.)

Constellation
In the CMMI architecture, a collection of components that are used to construct models, training materials, and appraisal materials in an area of interest (e.g., services and development).

Container (information asset container)
A physical or logical location where assets are stored, transported, and processed. A container can encompass technical containers (servers, network segments, personal computers), physical containers (paper, file rooms, storage spaces, or other media such as CDs, disks, and flash drives), and people (including people who might have detailed knowledge about the information asset). [KIM]

Continuity of operations
An organization's ability to sustain assets and services in light of realized risk. Typically used interchangeably with *service continuity*. [RISK] [SC] (See the related term *Service Continuity*.)

Controls
The methods, policies, and procedures—manual or automated—that are adopted by an organization to ensure the safeguarding of assets, the accuracy and reliability of management information and financial records, the promotion of administrative efficiency, and adherence to standards. [CTRL] [KIM]

Controls Management (CTRL)
An engineering process area in CERT-RMM. The purpose of Controls Management is to establish, implement, monitor, and manage an internal control system that ensures the effectiveness and efficiency of operations through mission assurance of high-value services.

Convergence
The harmonization of operational risk management activities that have similar objectives and outcomes.

Corrective maintenance
A process of correcting and repairing problems that degrade the operational capability of facility services. [EC]

Cost of resilience
An accumulation of expense and capital costs related to providing resilience services and achieving resilience requirements. [FRM]

Credentialing
A process for identifying, acquiring, and maintaining access for first responders (vital staff members) from governmental authorities. [PM]

Crisis
An incident in which the impact on the organization is imminent or immediate. A crisis requires immediate organizational action because the effect of the incident is already felt by the organization and must be limited or contained. [IMC]

Critical success factors
The key areas in which favorable results are necessary to achieve goals. They are both internal and external to the organization. They can originate in the organization's particular industry and with its peers, in its operating environment, from temporary barriers, challenges, or problems, or from the various domains of organizational management. [EF]

Cross-training
Training in different roles or responsibilities within the organization, thus preparing staff to accept and perform new roles, however temporary, until a return to business as usual can be accomplished. [PM]

Cryptographic controls
Encryption of data and information that provides an additional layer of control over information assets by ensuring that access is limited to those who have the appropriate deciphering keys. [KIM]

Custodian
See *asset custodian*.

Defined process
A managed process that is tailored from the organization's set of standard processes according to the organization's tailoring guidelines; has a maintained process description; and contributes work products, measures, and other process improvement information to organizational process assets. [OPD] (See the related terms *managed process* and *organization's set of standard processes*.)

Deprovisioning
The process of revoking or removing an identity's access to organizational assets. [AM] (See the related term *provisioning*.)

Derived measures
Data obtained by combining two or more base measures (for example, the percentage of risk mitigation plans completed on time in the last 12 months). [MA]

Disposition
The appropriate and proper retirement of an asset at the end of its useful life. [KIM] [RISK]

Encryption policies
Policies that govern the use of cryptographic technologies as appropriate or required for each level of information asset categorization. Includes organizational policies that manage the assignment of use, storage, disposal, and protection of cryptographic keys (such as public and private keys). [KIM]

Enterprise
Synonymous with *organization*.

Enterprise Focus (EF)
An enterprise process area in CERT-RMM. The purpose of Enterprise Focus is to establish sponsorship, strategic planning, and governance over the operational resilience management system.

Enterprise-level resilience requirement
Resilience requirements that reflect enterprise-level needs, expectations, and constraints. These requirements affect nearly all aspects of an organization's operations. [RRD]

Environmental Control (EC)
An operations process area in CERT-RMM. The purpose of Environmental Control is to establish and manage an appropriate level of physical, environmental, and geographical controls to support the resilient operations of services in organizational facilities.

Establish and maintain
Whenever "establish and maintain" (or "established and maintained") is used as a phrase, it refers not only to the development and maintenance of the object of the practice (such as a policy) but to the documentation of the object and observable usage of the object. For example, "Formal agreements with external entities are established and maintained" means that not only are the agreements formulated, but they also are documented, have assigned ownership, and are maintained relative to corrective actions, changes in requirements, or improvements.

Event
One or more occurrences that affect organizational assets and have the potential to disrupt operations. [IMC] (See the related term *incident*.)

Event triage
The process of categorizing, correlating, and prioritizing events with the objective of assigning events to incident handling and response. [IMC]

Exercise
The testing of a service continuity plan on a regular basis to ensure that it will achieve its stated objectives when executed as the result of a disruption or interruption. [SC]

Expected component
A model component that explains what may be done to satisfy a required CERT-RMM component. Specific and generic practices are expected model components. Model users can implement the expected components explicitly or implement equivalent alternative practices. (See the related terms *informative component* and *required component*.)

External Dependencies Management (EXD)
An operations process area in CERT-RMM. The purpose of External Dependencies Management is to establish and manage an appropriate level of controls to ensure the resilience of services and assets that are dependent on the actions of external entities.

External dependency
An external dependency exists when an external entity has access to, control of, ownership in, possession of, responsibility for, or other defined obligations related to one or more assets or services of the organization. [EXD] (See the related term *external entity*.)

External entity
An individual, business, or business unit (such as a customer, a contractor, or another group within the same enterprise) that is external to and in a supporting or influencing relationship with the organization that is using a process area. [EXD]

Facility
Any tangible and physical asset that is part of the organization's physical plant. Facilities include office buildings, warehouses, data centers, and other physical structures. [ADM] [EC]

Federation
The assembled identity of an object across organizational units, organizations, systems, or other domains where the object has multiple identities. [ID]

Financial Resource Management (FRM)
An enterprise process area in CERT-RMM. The purpose of Financial Resource Management is to request, receive, manage, and apply financial resources to support resilience objectives and requirements.

First responder
Vital staff trained to conduct damage assessment after a disruption and recommend a path to reestablishing the high-value services of the organization. [PM]

Functional monitoring requirements
Requirements that describe, at a detailed level, what must be performed to meet the monitoring requirement. Specific infrastructure needs are a type of functional monitoring requirement. [MON]

Fuzz testing
A means of testing that causes a software program to consume deliberately malformed data to see how the program reacts [Microsoft 2009]. [RTSE]

Generic goal
A required model component that describes characteristics that must be present to institutionalize processes that implement a process area. (See the related term *institutionalization*.)

Generic practice
An expected model component that is considered important in achieving the associated generic goal. The generic practices associated with a generic goal describe the activities that are expected to result in achievement of the generic goal and contribute to the institutionalization of the processes associated with a process area.

Generic practice elaboration
An informative model component that appears after a generic practice to provide guidance on how the generic practice should be applied to the process area.

Geographical dispersion
The specific and planned dispersion or scattering of physical structures and facilities so that they are not all affected by a single event or incident. [EC]

Governance
An organizational process of providing strategic direction for the organization while ensuring that it meets its obligations, appropriately manages risk, and efficiently uses financial and human resources. [EF]

High-value assets
People, information, technology, or facilities upon whose confidentiality, integrity, availability, and productivity a high-value service depends. [ADM]

High-value services
Services upon which the success of the organization's mission depends. [EF] [RRD]

Human Resource Management (HRM)
An enterprise process area in CERT-RMM. The purpose of Human Resource Management is to manage the employment life cycle and performance of staff in a manner that contributes to the organization's ability to manage operational resilience.

Identity
Documentation of certain information about a person, object, or entity that may require access to organizational assets to fulfill its role in executing services. [ID]

Identity community
The baseline population of persons, objects, and entities—internal and external to the organization—that could be or are authorized to access and use organizational assets commensurate with their job responsibilities and roles. Also, the collection of the organization's identity profiles. [ID]

Identity Management (ID)
An operations process area in CERT-RMM. The purpose of Identity Management is to create, maintain, and deactivate identities and associated attributes that provide access to organizational assets.

Identity management
A process that addresses the management of the life cycle of objects (typically people, but often systems, devices, or other processes) that need some level of trusted access to organizational assets. [ID]

Identity profile
Documentation of all of the relevant information necessary to describe the unique attributes, roles, and responsibilities of the associated person, object, or entity. [ID]

Identity registration
The process of making an identity "known" to the organization as a person, object, or entity that may require access to organizational assets and that may have to be authenticated and authorized to use access privileges. [ID]

Identity repository
A common accessible information repository that provides a single (or virtual) consistent source of information about organizational identities. [ID]

Impact area (organizational impact area)
An area in which criteria are established to determine and express the potential impact of realized risk on the organization. Typical impact areas include life and safety of employees and customers, financial, legal, and productivity. [RISK]

Impact valuation
Determines the extent of the impact of operational risk using the organization's risk measurement criteria. [RISK]

Incident
An event (or series of events) of higher magnitude that significantly affects organizational assets and requires the organization to respond in some way to prevent or limit organizational impact. [IMC]

Incident closure
The retirement of an incident that has been responded to (i.e., there are no further actions required, and the organization is satisfied with the result) and for which the organization has performed a formal post-incident review. [IMC]

Incident escalation
The process of notifying relevant stakeholders about an incident that requires an organizational response and involves stakeholder actions to implement, manage, and bring to closure with an appropriate and timely solution. [IMC]

Incident life cycle
The life cycle of an incident from detection to closure. Collectively, the processes of logging, tracking, documenting, escalating and notifying, gathering and preserving evidence, and closing incidents. [IMC]

Incident Management and Control (IMC)
An operations process area in CERT-RMM. The purpose of Incident Management and Control is to establish processes to identify and analyze events, detect incidents, and determine an appropriate organizational response.

Incident owner
The individuals or teams to whom an incident is assigned for containment, analysis, and response. [IMC]

Incident response
The actions the organization takes to prevent or contain the impact of an incident to the organization while it is occurring or shortly after it has occurred. [IMC]

Incident stakeholder
A person or organization with a vested interest in the management of an incident throughout its life cycle. [IMC]

Information asset
Information or data that is of value to the organization, including diverse information such as patient records, intellectual property, customer information, and contracts. [ADM] [KIM]

Information asset baseline
A foundational configuration of an information asset from which changes to the asset can be detected over its life cycle. [KIM]

Information asset categorization
A process for labeling and handling the sensitivity of information assets, typically based on a categorization taxonomy or scheme. [KIM]

Information asset container
A technical or physical asset upon which information is stored, transported, or processed, or a person who has information or knowledge. [ADM] [KIM]

Information asset owner
See the related term *asset owner*.

Informative component
A model component that helps model users understand required and expected components. Informative components can contain examples, detailed explanations, or other helpful information. Subpractices, notes, references, goal titles, practice titles, sources, typical work products, amplifications, and generic practice elaborations are informative model components. (See the related terms *expected component* and *required component*.)

Institutionalization
Incorporation into the ingrained way of doing business that an organization follows routinely as part of its corporate culture.

Integrity
For an asset, the quality of being in the condition intended by the owner and therefore continuing to be useful for the purposes intended by the owner. [KIM] [TM]

Intellectual property
The unique information assets of the organization that are created by the organization and are vital to its success. Intellectual property may include trade secrets, formulas, trademarks, and other organizationally-produced assets. [KIM]

Internal control system
The methods, policies, and procedures used to protect and sustain high-value assets at a level commensurate with their role in supporting organizational services. [CTRL] (See the related term *high-value assets*.)

Key control indicators
Organizationally specific indicators that provide information about the effectiveness of the organization's internal control system. [CTRL]

Key performance indicators
Organizationally specific performance metrics that measure progress against the organization's strategic objectives and critical success factors. [EF]

Key risk indicators
Organizationally specific thresholds that, when crossed, indicate levels of risk that may be outside of the organization's risk tolerance. [EF] [RISK]

Knowledge and Information Management (KIM)
An operations process area in CERT-RMM. The purpose of Knowledge and Information Management is to establish and manage an appropriate level of controls to support the confidentiality, integrity, and availability of the organization's information, vital records, and intellectual property.

Level of control
The extent to which administrative, physical, or technical controls have been applied to an asset. This might indicate the mix or number of controls applied to the asset in response to types of resilience requirements (confidentiality, integrity, availability) or the rigor or degree of controls (such as levels of control between ad hoc version control and formal configuration management).

Line of business
A logical grouping of organizational units that have a common purpose, such as production of products or delivery of services for a particular market segment.

Managed process
A performed process that is planned and executed in accordance with policy; employs skilled people having adequate resources to produce controlled outputs; involves relevant stakeholders; is monitored, controlled, and reviewed; and is evaluated for adherence to its process description. (See the related term *performed process*.)

Measurement and Analysis (MA)
A process management process area in CERT-RMM. 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.

Measurement objectives
Documents the purpose for which measurements and analysis are done and specifies the kinds of actions that may be taken based on the results of data analysis. [MA]

Measures
Measurements of the resilience process that may be categorized by obtaining direct measurements (*base measures*) or by obtaining measurements that are a combination of two or more base measures (*derived measures*). [MA]

Misuse/abuse case
A descriptive statement of the undesirable, non-standard conditions that software is likely to face during its operation from either unintentional misuse or intentional and malicious misuse or abuse. [RTSE]

Model scope
The parts of CERT-RMM that will be used to guide the improvement effort.

Monitoring (MON)
A process management process area in CERT-RMM. The purpose of Monitoring is to collect, record, and distribute information about the operational resilience management system to the organization on a timely basis.

Monitoring infrastructure
The technologies and support services that are needed to support the achievement of monitoring requirements. [MON]

Monitoring requirements
The requirements established to determine the information gathering and distribution needs of stakeholders. [MON]

Monitoring stakeholder
A person or group with a vested interest in being involved in or a beneficiary of the organization's monitoring activities. [MON]

Operational constraint
A limit imposed on an organization's operational activities. Such a limit can be imposed by the organization on itself or can come from the organization's operating environment (e.g., regulations). [RRD]

Operational resilience
The emergent property of an organization that can continue to carry out its mission in the presence of operational stress and disruption that does not exceed its operational limit. (See the related term *operational risk*.)

Operational resilience management
The direction and coordination of activities to achieve resilience objectives that align with the organization's strategic objectives and critical success factors.

Operational resilience management system
The mechanism through which operational resilience management is performed. The "system" includes the plan, program, processes, procedures, practices, and people that are necessary to manage operational resilience.

Operational resilience requirements
Refers collectively to requirements that ensure the protection of high-value assets as well as their continuity when a disruptive event has occurred. The requirements traditionally encompass security, business continuity, and IT operational requirements. These include the security objectives for information assets (confidentiality, integrity, and availability) as well as the requirements for business continuity planning and recovery and the availability and support requirements of the organization's technical infrastructure. [RRD]

Operational risk
The potential impact on assets and their related services that could result from inadequate or failed internal processes, failures of systems or technology, the deliberate or inadvertent actions of people, or external events.

Operational risk taxonomy
The collection and cataloging of common operational risks that the organization is subject to and must manage. The risk taxonomy is a means for communicating these risks and for developing mitigation actions specific to an organizational unit or line of business if operational assets and services are affected by them. [RISK]

Organization
An administrative structure in which people collectively manage one or more services as a whole, and whose services share a senior manager and operate under the same policies. May consist of many organizations in many locations with different customers. (See the related terms *enterprise* and *organizational unit*.)

Organization's process asset library
A library of information used to store and make available process assets that are useful to those who are defining, implementing, and managing processes in the organization. This library contains process assets that include process-related documentation such as policies, defined processes, checklists, lessons-learned documents, templates, standards, procedures, plans, and training materials.

Organization's set of standard processes
A collection of definitions of the processes that guide activities in an organization. These process descriptions cover the fundamental process elements (and their relationships to each other, such as ordering and interfaces) that must be incorporated into the defined processes that are implemented in projects across the organization. A standard process enables consistent development and maintenance activities across the organization and is essential for long-term stability and improvement. [OPD] (See the related terms *defined process* and *process element*.)

Organizational asset
See *asset*.

Organizational impact area
See *impact area*.

Organizational process assets
Artifacts that relate to describing, implementing, and improving processes (e.g., policies, measurements, process descriptions, and process implementation support tools). The term *process assets* is used to indicate that these artifacts are developed or acquired to meet the business objectives of the organization, and they represent investments by the organization that are expected to provide current and future business value. (See the related term *process asset library*.)

Organizational Process Definition (OPD)
A process management process area in CERT-RMM. The purpose of Organizational Process Definition is to establish and maintain a usable set of organizational process assets and work environment standards for operational resilience.

Organizational Process Focus (OPF)
A process management process area in CERT-RMM. The purpose of Organizational Process Focus is to plan, implement, and deploy organizational process improvements based on a thorough understanding of current strengths and weaknesses of the organization's operational resilience processes and process assets.

Organizational process maturity
In models with a staged representation, organizational process maturity is measured by the degree of process improvement across predefined sets of process areas. Since CERT-RMM does not have a staged representation, characterization of organizational process maturity can only be implied by reaching successively higher levels of capability across CERT-RMM process areas.

Organizational scope
The part of the organization that is the focus of the CERT-RMM deployment.

Organizational sensitivity
The degree to which access to an information asset must be limited due to confidentiality or privacy requirements. [ADM]

Organizational subunit
Any sub-element of an organizational unit. An organizational subunit is fully contained within the organizational unit.

Organizational superunit
Any part of an organization that is at a higher level than the organizational unit. *Organizational superunit* can also be used to refer to the entire organization.

Organizational Training and Awareness (OTA)
An enterprise process area in CERT-RMM. The purpose of Organizational Training and Awareness is to promote awareness and develop skills and knowledge of people in support of their roles in attaining and sustaining operational resilience.

Organizational unit
A distinct subset of an organization or enterprise. An organizational unit is typically part of a larger organization, although in a small organization the organizational unit may be the whole organization.

Organizationally high-value services
See *high-value services*.

People
All staff, both internal and external to the organization, and all managers employed in some manner by the organization to perform a role or fulfill a responsibility that contributes to meeting the organization's goals and objectives. [PM]

People Management (PM)
An operations process area in CERT-RMM. The purpose of People Management is to establish and manage the contributions and availability of people to support the resilient operation of organizational services.

Perfective maintenance
Maintenance performed by acquiring additional or improved operational capacity. [EC]

Performed process
A process that accomplishes the needed work to produce work products. The specific goals of the process area are satisfied.

Physical control
A type of control that prevents physical access to and modification of information assets or physical access to technology and facilities. Physical controls often include such artifacts as card readers and physical barrier methods. [EC] [KIM] [TM]

Planned downtime
Acceptable and planned interruption of the availability of an information or technology asset, usually as the result of a user- or management-initiated event. [TM]

Post-incident review
A formal part of the incident closure process that refers to the organization's formal examination of the causes of an incident and the ways in which the organization responded to it, as well as the administrative, technical, and physical control weaknesses that may have allowed the incident to occur. [IMC]

Preventive maintenance
Preplanned activities performed to prevent potential facility problems from occurring. [EC]

Privacy
The assurance that information about an individual is disclosed only to people, processes, and devices authorized by that individual or permitted under privacy laws and regulations. [KIM]

Privilege
See *access privilege*.

Problem management
The process that an organization uses to identify recurring problems, examine root causes, and develop solutions for these problems to prevent future, similar incidents. [IMC]

Process
Activities that can be recognized as implementations of practices in the model. These activities can be mapped to one or more practices in process areas to allow the model to be useful for process improvement and process appraisal. (See the related terms *process area*, *subprocess*, and *process element*.)

There is a special use of the phrase “the process” in the statements and descriptions of the generic goals and generic practices. In that context, “the process” is the process or processes that implement the process area.

Process architecture
The ordering, interfaces, interdependencies, and other relationships among the process elements in a standard process. Process architecture also describes the interfaces, interdependencies, and other relationships between process elements and external processes (e.g., contract management). [OPD]

Process area
A cluster of related practices in an area that, when implemented collectively, satisfy a set of goals considered important for making improvement in that area.

Process asset library
A collection of process asset holdings that can be used by an organization or project. (See the related term *organization’s process asset library*.)

Process capability
The range of expected results that can be achieved by following a process. The generic goals and practices define the degree to which a process is institutionalized; capability levels indicate the degree to which a process is institutionalized.

Process element
The fundamental unit of a process. A process can be defined in terms of subprocesses or process elements. A subprocess can be further decomposed into subprocesses or process elements; a process element cannot. Each process element covers a closely related set of activities (e.g., estimating element, peer review element). Process elements can be portrayed using templates to be completed, abstractions to be refined, or descriptions to be modified or used. A process element can be an activity or a task. [OPD] (See the related term *subprocess*.)

Process performance
A measure of actual results achieved by following a process. It is characterized by both process measures (e.g., vulnerabilities eliminated before being exploited) and product or

service measures (e.g., control system network unavailability due to exploited vulnerabilities).

Protection strategy
The strategy, related controls, and activities necessary to protect an asset from undesired harm or disruptive events. The protection strategy is relative to the conditions to which the asset is subjected. (See the related term *condition*.)

Provisioning
The process of assigning or activating an identity profile and its associated roles and access privileges. [ID]

Proximity
The relative distance between facilities, which is a consideration in co-location and geographical dispersion. [EC] (See the related terms *co-location* and *geographical dispersion*.)

Public infrastructure
Infrastructure owned by the community in the geographical area that contains a facility. Includes telecommunications and telephone services; electricity, natural gas, and other energy sources; water and sewer services; trash collection and disposal; and other support services. [EC]

Public services
Services that are provided in the community or in the geographical area that contains a facility. Includes fire response and rescue services; local and federal law enforcement; emergency management services such as paramedics and first responders; and animal control. [EC]

Recovery point objective (RPO)
Establishes the point to which an information or technology asset (typically an application system) must be restored to allow recovery of the asset and associated services after a disruption. [SC]

Recovery time objective (RTO)
Establishes the period of acceptable downtime of an information or technology asset after which the organization would suffer an unwanted consequence or impact. [SC]

Regulation
A type of compliance obligation issued by a governmental, regulatory, or other agency. [COMP]

Release build
A version of an information or technology asset that is to be released into production; an object in the release management process. [TM]

Release management
The process of managing successive release of versions of information and technology assets into an operations and production environment. [TM]

Relevant stakeholder
A stakeholder that is identified for involvement in specified activities and is included in a plan. (See the related term *stakeholder*.)

Required component
A CERT-RMM component that is essential to achieving process improvement in a given process area. Required components are used in appraisals to determine process capability. Specific goals and generic goals are required components. (See the related terms *expected component* and *informative component*.)

Residual risk
The risk that remains and is accepted by the organization after response plans are implemented. [RISK]

Resilience
The physical property of a material by which it can return to its original shape or position after deformation that does not exceed its elastic limit [http://wordnet.princeton.edu]. (See the related term *operational resilience*.)

Resilience budget
A budget specifically developed and funded to support the organization's resilience activities. [FRM]

Resilience-focused asset
An asset that is specifically designated to support the organization's resilience activities, such as a secondary data center used when a disruption affects the operation of a primary data center.

Resilience management
See *operational resilience management*.

Resilience obligations
An understanding of a commitment, promise, or duty to follow and enforce the resilience requirements of the organization. [HRM]

Resilience requirement
For an asset, a characteristic or capability that it must possess or a condition that it must meet to ensure that it remains viable and sustainable as needed to support a service. More generally, a need, expectation, or obligation that the organization establishes to ensure resilience.

Resilience Requirements Development (RRD)
An engineering process area in CERT-RMM. The purpose of Resilience Requirements Development is to identify, document, and analyze the operational resilience requirements for high-value services and related assets.

Resilience Requirements Management (RRM)
An engineering process area in CERT-RMM. The purpose of Resilience Requirements Management is to manage the resilience requirements of high-value services and

associated assets and to identify inconsistencies between these requirements and the activities that the organization performs to meet the requirements.

Resilience specifications
Criteria that the organization establishes for a working relationship with an external entity, which may be incorporated into contractual terms. Typically include the resilience requirements of any of the organization's high-value assets and services that are placed in the external entity's control. Also may include required characteristics of the external entity (e.g., financial condition and experience), required behaviors of the external entity (e.g., security and training practices), and performance parameters that must be exhibited by the external entity (e.g., recovery time after an incident and response time to service calls).

Resilience staff
Internal or external staff who are specifically involved in or assigned to resilience-focused activities that are typically found in security, business continuity, and IT operations disciplines.

Resilience training
The process and activities focused on imparting the necessary skills and knowledge to people for performing their roles and responsibilities in support of the organization's operational resilience management system. [OTA]

Resilience training needs
Training requirements related to the skills and competencies required at a tactical level to carry out the activities required for managing operational resilience. [OTA]

Resilient Technical Solution Engineering (RTSE)
An engineering process area in CERT-RMM. The purpose of Resilient Technical Solution Engineering is to ensure that software and systems are developed to satisfy their resilience requirements.

Return on resilience investment (RORI)
The return on investment for funding resilience activities. Provides a way to justify resilience costs and provides direct support for the contribution that managing operational resilience makes toward achieving strategic objectives. [FRM]

Risk
The possibility of suffering harm or loss. From a resilience perspective, risk is the combination of a threat and a vulnerability (condition), the impact (consequence) on the organization if the vulnerability is exploited, and the presence of uncertainty. In CERT-RMM, this definition is typically applied to the asset or service level such that risk is the possibility of suffering harm or loss due to disruption of high-value assets and services. [RISK]

Risk analysis
A risk management process focused on understanding the condition and consequences of risk, prioritizing risks, and determining a path for addressing risks. Determines the

importance of each identified operational risk and is used to facilitate the organization's risk disposition and mitigation activities. [RISK]

Risk appetite
An organization's stated level of risk aversion. Informs the development of risk evaluation criteria in impact areas for the organization. [RISK] (See the related terms *impact area* , *risk measurement criteria*, and *risk tolerance*.)

Risk category
An organizationally defined description of risk that typically aligns with the various sources of operational risk but can be tailored to the organization's unique risk environment. Risk categories provide a means to collect and organize risks to assist in the analysis and mitigation processes. [RISK]

Risk disposition
A statement of the organization's intention for addressing an operational risk. Typically limited to "accept," "transfer," "research," or "mitigate." [RISK]

Risk Management (RISK)
An enterprise process area in CERT-RMM. The purpose of Risk Management is to identify, analyze, and address risks to organizational assets that could adversely affect the operation and delivery of services.

Risk management
The continuous process of identifying, analyzing, and addressing risks to organizational assets that could adversely affect the operation and delivery of services. [RISK]

Risk measurement criteria
Objective criteria that the organization uses for evaluating, categorizing, and prioritizing operational risks based on impact areas. [RISK] (See the related term *impact area*.)

Risk mitigation
The act of reducing risk to an acceptable level. [RISK]

Risk mitigation plan
A strategy for mitigating risk that seeks to minimize the risk to an acceptable level. [RISK]

Risk parameter (risk management parameter)
Organizationally specific risk tolerances used for consistent measurement of risk across the organization. Risk parameters include risk tolerances and risk measurement criteria. [RISK] (See the related terms *risk tolerance* and *risk measurement criteria*.)

Risk statement
A statement that clearly articulates the context, conditions, and consequences of risk. [RISK]

Risk taxonomy
See *operational risk taxonomy*.

Risk threshold
An organizationally developed type of risk parameter that is used by management to determine when a risk is in control or when it has exceeded acceptable organizational limits. [RISK]

Risk tolerance
Thresholds that reflect the organization's level of risk appetite by providing levels of acceptable risk in each operational risk category that the organization has established. Risk tolerance, as a risk parameter, also establishes the organization's philosophy on risk management—how risks will be controlled, who has the authorization to accept risk on behalf of the organization, and how often and to what degree operational risk should be assessed. [RISK]

Root-cause analysis
An approach for determining the underlying causes of events or problems as a means of addressing the symptoms of such events as they manifest in organizational disruptions. [VAR]

Scope
See *appraisal scope*, *model scope*, and *organizational scope*.

Secure design pattern
A general, reusable solution to a commonly occurring problem in design. A design pattern is not a finished design that can be transformed directly into code. It is a description or template for how to solve a problem that can be used in many different situations. Secure design patterns are meant to eliminate the accidental insertion of vulnerabilities into code or to mitigate the consequences of vulnerabilities. They address security issues at widely varying levels of specificity, ranging from architectural-level patterns involving the high-level design of the system down to implementation-level patterns providing guidance on how to implement portions of functions or methods in the system [Dougherty 2009]. [RTSE]

Sensitivity
A measure of the degree to which an information asset must be protected based on the consequences of its unauthorized access, modification, or disclosure. [KIM]

Service
A set of activities that the organization carries out in the performance of a duty or in the production of a product. [ADM] [EF] (See the related term *business process*.)

Service Continuity (SC)
An engineering process area in CERT-RMM. The purpose of Service Continuity is to ensure the continuity of essential operations of services and related assets if a disruption occurs as a result of an incident, disaster, or other disruptive event.

Service continuity plan (business continuity plan)
A service-specific plan for sustaining services and associated assets under degraded conditions. [SC]

Service level agreement (SLA)
A type of agreement that specifies levels of service expected from business partners in the performance of a contract or agreement. In CERT-RMM, SLAs are expanded to include the satisfaction of resilience requirements by business partners when one or more organizational assets are in their custodial care.

Service-level resilience requirements
Service requirements established by owners of a service such as an organizational unit or a line of business. [RRD] (See the related term *asset-level resilience requirements*.)

Service profile
A description of services in sufficient detail to capture the activities, tasks, and expected outcomes of the services and the assets that are vital to the service. [EF]

Service resilience requirements
Resilience needs of a service in its pursuit of its mission. Resilience requirements for services primarily address availability and recoverability but are also directly related to the confidentiality, integrity, and availability requirements of associated assets. [RRD]

Services map
Details the relationships between a service, associated business processes, and associated assets. [RRD]

Shared resilience requirements
Requirements that are developed for shared organizational assets such as a facility in which more than one high-value service is executed. [RRD]

Skills inventory or repository
A means for identifying and documenting the current skill set of the organization's human resources. [HRM]

Specific goal
A required model component that describes the unique characteristics that must be present to satisfy the process area. (See the related terms *process area* and *required component*.)

Specific practice
An expected model component that is considered important in achieving the associated specific goal. The specific practices describe the activities expected to result in achievement of the specific goals of a process area. (See the related terms *expected component*, *process area*, and *specific goal*.)

Staff
All people, both internal and external to the organization, employed in some manner by the organization to perform a role or fulfill a responsibility that contributes to meeting the organization's goals and objectives. Does not include those in managerial roles.

Stakeholder
A person or organization that has a vested interest in the organization or its activities. (See the related terms *communications stakeholder*, *monitoring stakeholder*, and *relevant stakeholder*.)

Standard process
An operational definition of the basic process that guides the establishment of a common process in an organization. A standard process describes the fundamental process elements that are expected to be incorporated into any defined process. It also describes relationships (e.g., ordering, interfaces) among these process elements. [OPD] (See the related term *defined process*.)

Strategic objectives (strategic drivers)
The performance targets that the organization sets to accomplish its mission, vision, values, and purpose. [EF]

Strategic planning
The process of developing strategic objectives and plans for meeting these objectives. [EF]

Subprocess
A process that is part of a larger process. A subprocess can be decomposed into subprocesses or process elements. [OPD] (See the related terms *process* and *process element*.)

Succession planning
A form of continuity planning for vital staff and/or decision-making managers focused on providing a smooth transition for vital roles and sustaining the high-value services of the organization. [PM]

Supplier
An internal or external organization or contractor that supplies key products and services to the organization to contribute to accomplishing the missions of its high-value services.

Sustain
Maintain in a desired operational state.

Sustainment strategy
The strategy, related controls, and activities necessary to sustain an asset when it is subjected to undesired harm or disruptive events. The sustainment strategy is relative to the consequences to the organization if the asset is harmed or disrupted.

Technical control
A type of technical mechanism that supports protection methods for assets such as firewalls and electronic access controls. [KIM] [TM]

Technology asset
Any hardware, software, or firmware used by the organization in the delivery of services. [TM]

Technology interoperability
The ability of technology assets to exist and operate in a connected manner to meet an organizational goal, objective, or mission. [TM]

Technology Management (TM)
An operations process area in CERT-RMM. The purpose of Technology Management is to establish and manage an appropriate level of controls related to the integrity and availability of technology assets to support the resilient operations of organizational services.

Threat
The combination of a vulnerability, a threat actor, a motive (if the threat actor is a person or persons), and the potential to produce a harmful outcome for the organization. [VAR] (See the related term *condition*.)

Threat actor
A situation, entity, individual, group, or action with the potential to exploit a threat. [VAR]

Threat environment
The set of all types of threats that could affect the current operations of the organization. (See the related term *threat*.)

Threat motive
The reason that a threat actor would exploit a vulnerability or otherwise cause harm. [VAR]

Unplanned downtime
Interruption in the availability of an information or technology asset (and in some cases a facility asset) due to an unplanned event or incident, often resulting from diminished operational resilience. [TM]

User
Any entity or object to which the organization has granted some form of access to an organizational asset. Typically referred to as an “identity.” (See the related term *identity*.)

Vital records
Records that must be preserved and available for retrieval if needed. This refers to records or documents that, for legal, regulatory, or operational reasons, cannot be irretrievably lost or damaged without materially impairing the organization’s ability to conduct business. [KIM]

Vital staff
A select group of individuals who are absolutely essential to the sustained operation of the organization, particularly under stressful conditions. [PM]

Vulnerability
An exposure, flaw, or weakness that could be exploited. The susceptibility of an organizational service or asset to disruption. [VAR]

Vulnerability Analysis and Resolution (VAR)
An operations process area in CERT-RMM. The purpose of Vulnerability Analysis and Resolution is to identify, analyze, and manage vulnerabilities in an organization's operating environment.

Vulnerability management strategy
A strategy for identifying and reducing exposure to known vulnerabilities. [VAR]

Vulnerability repository
An organizational inventory of known vulnerabilities. [VAR]

Vulnerability resolution
The action that the organization takes to reduce or eliminate exposure to vulnerability. [VAR]

Waiver
Documentation for staff members who have been exempted from awareness training or other activities for any reason. Such documentation includes the rationale for the waiver and approval by the individual's manager (or similarly appropriate person). Each required course should include criteria for granting training waivers. [OTA]