Software Engineering Institute

CERT® Resilience Management Model, Version 1.2

Organizational Training and Awareness (OTA)

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

ORGANIZATIONAL TRAINING AND AWARENESS

Enterprise

Purpose

The purpose of Organizational Training and Awareness is to promote awareness in and develop skills and knowledge of people in support of their roles in attaining and sustaining operational resilience.

Introductory Notes

Organizational Training and Awareness is an enterprise process area that seeks to ensure that the organization's staff are aware of resilience needs and concerns and that they behave in a manner consistent with the organization's operational resilience requirements and goals. This requires that they be made aware of the organization's resilience plans and programs and that they understand their role in these plans and programs. Staff must also be provided specialized training on a regular basis that establishes resilience as an organizational competency and encourages improvement in skill sets relative to their specific or general roles in managing operational resilience.

Organizational Training and Awareness focuses exclusively on skills, knowledge, and cognizance for resilience activities, not generalized training across the organization. However, these resilience training and awareness activities should integrate with and be supported by the organization's overall training and awareness program and plan. Specifically, training refers to imparting the necessary skills and knowledge to people for performing their roles and responsibilities in support of the organization's operational resilience management system. Awareness is aimed at focusing the attention of staff throughout the organization on resilience issues, concerns, policies, plans, and practices and increasing their cognizance of and acculturation to resilience. Training imparts skills and knowledge to enable staff to perform a specific resilience function; awareness activities create cognizance to bring about desired behaviors in support of the resilience process and to support a risk-aware culture in the organization.

An organizational training and awareness program is a comprehensive capability that typically includes the following activities:

- identifying the training and awareness needs of the organization
- sourcing training and awareness materials
- providing training and implementing awareness activities, using a variety of methods
- establishing and maintaining records of training and awareness activities
- evaluating the effectiveness of the training and awareness program
- revising the program to improve effectiveness and in response to changes in training and awareness needs

The Organizational Training and Awareness process area has four specific goals. The Establish Awareness Program goal addresses the creation, planning, and organization of an

awareness program. Conduct Awareness Activities puts awareness plans into action throughout the enterprise and evaluates their effectiveness. The Establish Training Capability goal addresses the creation, planning, and organization of a training capability. Conduct Training addresses the delivery and evaluation of training activities.

Organizational Training and Awareness is a complementary process area to the Human Resource Management and People Management process areas. Organizational Training and Awareness focuses on general awareness, skill building, and ongoing training. Human Resource Management is focused on managing the employment life cycle and performance of an employee in support of operational resilience. People Management identifies key staff and manages their availability to the services they support, ensuring the resilience of the "people" asset.

Related Process Areas

Managing the resilience of the people in the organization is performed in the People Management process area.

Managing the employment life cycle and performance of an employee in support of operational resilience is addressed in the Human Resource Management process area.

Awareness activities for external entities such as business partners and vendors are addressed in the External Dependencies Management process area.

Awareness communications are addressed in the Communications process area.

Tracking awareness activities for compliance purposes is addressed in the Compliance process area.

Guidance about tracking awareness activities for governance functions is addressed in the Enterprise Focus process area.

Summary of Specific Goals and Practices

Goals	Practices
OTA:SG1 Establish Awareness Program	OTA:SG1.SP1 Establish Awareness Needs
	OTA:SG1.SP2 Establish Awareness Plan
	OTA:SG1.SP3 Establish Awareness Delivery Capability
OTA:SG2 Conduct Awareness Activities	OTA:SG2.SP1 Perform Awareness Activities
	OTA:SG2.SP2 Establish Awareness Records
	OTA:SG2.SP3 Assess Awareness Program Effectiveness
OTA:SG3 Establish Training Capability	OTA:SG3.SP1 Establish Training Needs
	OTA:SG3.SP2 Establish Training Plan
	OTA:SG3.SP3 Establish Training Capability
OTA:SG4 Conduct Training	OTA:SG4.SP1 Deliver Training
	OTA:SG4.SP2 Establish Training Records
	OTA:SG4.SP3 Assess Training Effectiveness

Specific Practices by Goal

OTA:SG1 Establish Awareness Program

An awareness program that supports the organization's resilience program is established.

An awareness program is a means by which the organization can highlight important behaviors and begin the process of acculturating staff and external entities to important organizational goals, objectives, and critical success factors. Awareness differs significantly from skill-based training. Awareness focuses on communicating a message to gather support for an organizational imperative; skill-based training is aimed at imparting knowledge to staff that is necessary to perform a role or fulfill a responsibility. Awareness of resilience makes staff more cognizant of their role in supporting the organization's operational resilience management system and in ensuring adequate operational resilience for high-value services and assets.

To establish an effective awareness program, an organization must identify awareness needs and establish a plan and capability to meet those needs. Adjustments to the plan and the program are made over the course of time to address changes in needs and to make overall improvements.

OTA:SG1.SP1 Establish Awareness Needs

The awareness needs of the organization are established and maintained.

Awareness needs reflect the message that is to be communicated regarding resilience to all entities, internal and external, that have a vested interest in the resilience activities of the organization (referred to as "staff"). These may be derived from the organization's resilience strategic plans, policies, or other goal and objectives. Awareness needs are derived by determining the set of resilience topics, plans, issues, or policies of which various sets of the organization's population have to be kept aware. For many organizations, the awareness needs may be consistent across the organization's entire population; for others, different parts of the organization may have different awareness needs. If high-value business processes are outsourced, there may be awareness needs that span one or more external entities. All of these populations should be identified and their awareness needs documented.

Awareness needs are temporal and may change as a result of changes in technology, policy, strategy, and risks being managed. A routine process to maintain and update awareness needs should be put in place.

Sources of awareness needs include

- resilience requirements that specify how assets and services have to be protected and sustained
- organizational policies that attempt to enforce and reinforce acceptable behaviors or implement necessary controls across the enterprise, such as keeping payroll data confidential
- vulnerabilities under watch or that are being actively managed, such as email and internet viruses

- laws and regulations to which the organization is subject because of its industry, geographical location, or type of business, such as
  - confidentiality and privacy regulations
  - other federal, state, and local laws that restrict disclosure of information or modification of information
- service continuity and communications plans that are of importance to staff in being prepared to act in the event of an incident or disaster
- event reporting procedures that include instructions for when and to whom to report an event or incident

Typical work products

1. Stated objectives for awareness
2. List of staff members requiring awareness
3. Awareness needs for each staff group

Subpractices

1. Analyze the organization's operational resilience program to identify the types and extent of awareness efforts that are necessary to satisfy resilience program objectives.

   Because managing operational resilience requires acculturation of both internal and external entities (staff), the types and extent of awareness efforts may have to be extensive and rigorous. The objectives of awareness efforts must be clearly stated and must help the organization achieve staff acculturation to the organization's philosophy of managing operational resilience.

2. Document the awareness needs of the organization by staff group.

   Because managing operational resilience is a broad, enterprise-wide activity, awareness presentations may need to cover a broad range of topics and may require focused messages for particular staff groups. Awareness presentations must be purposefully aimed at communicating the appropriate message to each group.

3. Determine the resources necessary to meet the awareness needs.
4. Revise the awareness needs of the organization as changes to the resilience program and strategy are made.

OTA:SG1.SP2 Establish Awareness Plan

A plan for developing, implementing, and maintaining an awareness program is established and maintained.

The awareness plan details how the organization intends to carry out consistent and repeatable awareness efforts for each staff group. The plan must address the development, delivery, and maintenance of awareness presentations and materials to meet the awareness needs identified for each staff group. The plan should address near-term development and delivery and should be periodically adjusted based on new or changing needs and feedback from assessing the effectiveness of awareness activities.

Typical work products

1. Awareness plan
2. Documented commitments to the plan

Subpractices

1. Establish awareness plan content.

   Awareness plans typically include the following:

   - awareness needs and objectives
   - topics for awareness presentations and materials
   - identification of various staff groups and descriptions of how needs and topics vary by audience
   - schedules based on calendar-based and event-based awareness needs (An example of a calendar-based awareness need is "provide annual refresh training on login procedures and guidelines for choosing and managing secure passwords." An example of an event-based awareness need is "provide security and business continuity initiation briefing to new employees within ten days of starting work.")
   - methods to distribute awareness presentations and materials
   - requirements and quality standards for awareness presentations and materials, which may include identity guidelines for use of organizational trademarks
   - identification of awareness program roles and responsibilities
   - resource requirements

2. Establish commitments to the plan.

   Documented commitments by those responsible for implementing and supporting the plan are essential for the plan to be effective.

3. Determine resources necessary to carry out the plan.
4. Revise the plan and commitments as necessary.

OTA:SG1.SP3 Establish Awareness Delivery Capability

A capability for consistent and repeatable delivery of awareness artifacts is established and maintained.

The organization must be able to deliver awareness artifacts on a repeatable basis and ensure that the message communicated about operational resilience is consistent.

Establishing a capability for implementing the awareness plan requires the selection of appropriate awareness approaches, sourcing or developing awareness materials, obtaining appropriate awareness facilitators or instructors (if needed), delivering internal communications about awareness activities, and revising the awareness capability as needed.

Awareness activities for external entities such as business partners and vendors are addressed in the External Dependencies Management process area.

Typical work products

1. Awareness approaches by staff group
2. Awareness materials and supporting work products

Subpractices

1. Select the appropriate approaches to satisfy specific organizational awareness needs based on staff group.

   Many factors influence the selection of appropriate awareness approaches for the various segments of the organization's population. Typically, these include audience-specific roles, knowledge and daily behaviors, differences in work environment, budget, and consideration of organizational and work group culture. The selection of an approach should be based primarily on the best and most efficient means to create and support awareness for a given population, in light of any constraints.

   These are examples of awareness approaches:

   - distributing artifacts and workplace tools containing awareness messages (mouse pads, notepads, pens, mugs, hand tools, etc.)
   - poster campaigns
   - signage
   - newsletters—paper-based or electronic
   - email messages, letters, and memos from higher level managers
   - messages, reminders, and news items posted to internal web portals, electronic message boards, and physical bulletin boards
   - agenda items and supporting materials to be covered in organization-wide or team-based meetings
   - on-demand electronic briefings delivered via DVD or streaming network media
   - trainer-facilitated sessions delivered live or delivered remotely via teleconference, videoconference, or streaming network media
   - lunch seminars
   - acknowledgment or awards programs

2. Determine whether to develop the awareness materials internally, acquire them externally, or some combination.

   Criteria to consider when considering whether to develop awareness materials internally or to obtain the materials externally include

   - cost versus benefit
   - schedule and availability
   - availability of in-house expertise
   - availability and suitability of materials from qualified external entities

3. Develop or obtain awareness materials.

   These materials may contain sensitive information about incidents and other security events that can be used to raise general awareness about managing operational resilience. The organization should make provisions for adequately protecting this information from external entities that may be involved in awareness activities, either as providers or as participants.

Guidelines for establishing and maintaining relationships with external entities that serve as sources of awareness materials are addressed in the External Dependencies Management process area.

4. Develop or obtain qualified instructors or facilitators as needed.

   If instructor- or facilitator-led sessions are among the awareness activities that have been selected, qualified instructors or facilitators are required. To ensure that the instructors or facilitators have the necessary skills and knowledge to deliver the awareness materials, criteria can be established for evaluating candidates. For internal candidates, it may be necessary to provide specific training. For external resources, it is important to work with the provider to understand which of their staff will perform the work. This can be a factor in selecting or continuing to work with a specific provider.

5. Deliver internal communications about planned awareness activities.

   It may be appropriate to deliver communications about planned awareness activities. For example, if people are expected to attend events, communications about the schedule of the events are necessary. For some activities, it may be appropriate to inform higher level and other managers about the awareness plans and ask them to support and reinforce the plans by calling attention to the awareness activities in their regular communications or meetings with staff.

   Awareness communications are addressed in the Communications process area.

6. Revise the awareness materials and supporting artifacts as necessary.

   Situations in which awareness materials will have to be revised include

   - changes in existing awareness needs and requirements—for example, as a result of the implementation of a new procedure or technology
   - emergence of new awareness needs and requirements—for example, a new risk or vulnerability for which awareness is a suitable or necessary control
   - assessment of effectiveness of awareness presentations suggesting that awareness materials have to be changed
   - training refresh—for example, changing an awareness poster from time to time in order to be noticed by the intended audience

OTA:SG2 Conduct Awareness Activities

Awareness activities that support the organization's resilience program are performed.

The organization must perform awareness activities in order to carry out awareness plans and to fulfill the objectives of the awareness program. To ensure that awareness activities are being performed as prescribed, awareness activity records are established to track participation in awareness activities, and the effectiveness of the awareness activities is assessed.

OTA:SG2.SP1 Perform Awareness Activities

Awareness activities are performed according to the awareness plan.

Awareness activities implement the awareness approaches that the organization has considered and developed to meet the specific staff

needs. These activities can take many forms, as noted in the subpractices in OTA:SG1.SP3. Primarily, awareness activities will take the form of formal awareness presentations, but they could be supplemented by more continuous activities such as newsletters, email messages, or posters and other signage.

Awareness activities must meet the broad needs of staff members, and the logistics of performing these activities must be planned. The activities must be scheduled, advertised (if necessary), and resourced.

Typical work products

1. Awareness activity materials
2. Awareness activity schedules
3. Awareness activity logistics
4. List of staff responsible for each awareness activity

Subpractices

1. Determine the mix and frequency of awareness activities.
2. Plan and schedule awareness activities, including regular awareness presentations.
3. Perform logistics planning for each scheduled awareness activity.
4. Assign resources to each scheduled awareness activity.
5. Perform awareness activities according to the schedule and the plan.

   Awareness materials are distributed to the target populations according to the schedule and the approaches established in the plan.
6. Track the delivery of awareness activities against the plan and schedule.

OTA:SG2.SP2 Establish Awareness Records

Records of awareness activities performed are established and maintained.

Awareness activity records enable the organization to verify that awareness activities have been conducted according to plan. They provide evidence that staff and external entities have attended required activities appropriate for their job responsibility and role in the organization.

Records may also be necessary for compliance purposes to prove that the organization provides awareness presentations and requires staff and external entities to attend.

Recording awareness activities also facilitates evaluating activity effectiveness, particularly awareness presentations, through instruments such as evaluations and suggestion boxes.

The tracking of awareness activities for compliance purposes is addressed in the Compliance process area.

Guidance about tracking awareness activities for governance functions is addressed in the Enterprise Focus process area.

Typical work products

1. Awareness activity records
2. Awareness activity waivers

Subpractices

1. Keep records of all awareness activities conducted throughout the organization.

   These are examples of information that may be appropriate to record about awareness activities (not all of these would apply to every type of awareness activity):

   - a description of the specific awareness activity, when it occurred, and its duration
   - the population reached by an awareness activity
   - measures of participation, including specific records of attendance for awareness events
   - feedback received from participants

   If the awareness activity is required for certain staff groups or individual staff members, the organization should keep records for each attendee indicating whether or not the attendee completed the activity successfully.

   For staff who have been exempted from awareness activities for any reason, the organization should keep records documenting the rationale for the waiver, and the staff member's manager (or similarly appropriate person) should approve the waiver.

2. Make awareness activity records available to appropriate people or processes.

   Awareness activity records may be important in considering promotions or job assignments and thus should be made available to those who must make these types of decisions on a regular basis.

OTA:SG2.SP3 Assess Awareness Program Effectiveness

The effectiveness of the awareness program is assessed and corrective actions are identified.

A process should be implemented to evaluate the effectiveness of the awareness program by assessing how well program activities meet the awareness needs of the organization and staff.

Typically, assessing awareness program effectiveness occurs in the form of evaluations of awareness activities, but it may be a more challenging task for informal methods of awareness such as posters or regular communications.

These are examples of methods that can be used to evaluate the effectiveness of awareness activities:

- questionnaires or surveys designed to measure people's awareness of specific topics
- focus groups to elicit the awareness of a group of people after an awareness activity has occurred and to gather recommendations for awareness activity improvements

- selective interviews to inquire about awareness and any changes in behavior that may have occurred as a result of awareness activities
- behavioral measures to objectively evaluate shifts in the population's behavior after an awareness activity—for example, evaluating the strength of passwords before and after a password-awareness activity
- observations, evaluations, and benchmarking activities conducted by external entities

Typical work products

1. Evaluations of the awareness program and its activities
2. Awareness methods surveys
3. Focus group or interview results
4. Assessment results from staff (internal and external)

Subpractices

1. Assess staff awareness level based on the staff members' respective job responsibilities and roles.

   The purpose of this assessment is to determine whether awareness is sufficient to support the organization's resilience posture and program.

   For external entities that are being assessed, this should be included as part of the regular review of their contracts and performance.

2. Provide a mechanism for evaluating the effectiveness of each awareness activity with respect to the objectives for that activity.

   For awareness presentations, this mechanism should include evaluations of the material and the presenters.

3. Document suggested improvements to the awareness plan and program based on the evaluation of the effectiveness of the awareness activities.

OTA:SG3 Establish Training Capability

Training capabilities that support the operational resilience management system are established and maintained.

Training capability is established to provide focused and specific training to people who have roles and responsibilities that are focused on the operational resilience management system. The organization identifies the training needed to impart to people the necessary skills and knowledge to perform their roles and meet their responsibilities. A training plan is developed to guide the delivery of the training. Training materials and other resources are lined up to support the training plan.

Identifying staff with resilience roles and responsibilities, managing their performance, and conducting skills and knowledge gap analyses are addressed in the Human Resource Management process area.

OTA:SG3.SP1 Establish Training Needs

The training needs of the organization are established and maintained.

Resilience training needs reflect the skills and competencies required at a tactical level to carry out the activities required for managing operational resilience. These activities cover a broad range of disciplines, including security activities, business continuity, IT operations, and service delivery. As a result, the training needs for resilience staff tend to be vast and must seek not only to include these disciplines but to address the convergence of these disciplines toward the goal of actively managing resilience.

Training needs are established by identifying people in the organization with resilience roles and responsibilities and analyzing gaps in their knowledge and skills that have to be addressed in order for them to succeed in their resilience roles. Training needs should also be informed by the organization's resilience plan and strategy. *(Refer to the Enterprise Focus process area.)*

Some staff may have resilience roles only during times of stress or when the organization is responding to a disruption. It is important in the needs analysis process to account for these or any other secondary roles that people may have that are key to the resilience process but occur on a more discrete rather than continuous basis.

These are examples of sources of resilience training needs:

- the organization's resilience process and strategy
- the roles and responsibilities of staff in the traditional security, business continuity, and IT operations and service delivery domains
- the roles and responsibilities of staff involved in the operational resilience process management process (as described by the process areas in the CERT Resilience Management Model)
- the organization's vulnerability management process, which may highlight certain skills and knowledge that are required for the successful management of vulnerabilities
- the organization's human resource management process, which may identify training needs based on gap analysis of skills and knowledge, cross-training, and succession planning
- the process of service continuity, which may identify certain training needs associated with service continuity planning
- the organization's compliance management process, which may identify explicit training requirements based on legislation and other compliance obligations
- the organization's incident management process, which may identify training needs based on specific plans and practices for identifying and responding to incidents
- analyses of any assets that are accessed by or are in the possession of external entities and of business processes or services that are dependent on external entities, which may identify training needs for external entities

Skill inventories and gap analyses are explicitly addressed in the Human Resource Management process area.

Cross-training and training for succession planning are also addressed in the People Management process area and are key inputs for the training needs established in Organizational Training and Awareness.

Typical work products

1. Training needs

Subpractices

1. Collect information about skill gaps, cross-training, and succession planning by reviewing the job responsibilities of staff involved in resilience processes, as well as current performance levels.

   Input to this process may be derived from the processes in the Human Resource Management and People Management process areas.

2. Analyze the organization's resilience requirements, goals, and objectives to determine future training needs.
3. Determine the roles and skills necessary to perform the standard processes that constitute the operational resilience management system.
4. Document the resilience training needs of the organization.

   The training needs should focus not only on the skills and knowledge needed to perform particular roles in the supporting disciplines of security, business continuity, and IT operations and service delivery, but also on the convergence aspects of these disciplines toward operational resilience management. The training needs should also adequately cover the capabilities represented by the operational resilience management system.

5. Document the training necessary to perform the roles in the organization's set of standard operational resilience management processes.
6. Revise the resilience training needs of the organization as necessary.

OTA:SG3.SP2 Establish Training Plan

A plan for developing, implementing, and maintaining a resilience training program is established and maintained.

A tactical training plan is created to plan the development, delivery, and maintenance of training materials to meet the organization's resilience training needs. The plan should address near-term development and delivery and should be periodically adjusted in response to new or changing needs and to the assessment of effectiveness of training activities.

Typical work products

1. Resilience training plan
2. Documented commitments to the training plan

Subpractices

1. Establish resilience training plan content.

   Training plans typically include the following:

   - training needs
   - training topics

- schedules based on training activities and their dependencies
- methods used for training
- requirements and quality standards for training materials
- training tasks, roles, and responsibilities
- required resources, including tools, facilities, environments, staffing, and skills and knowledge

2. Establish commitments to the resilience training plan.

   Because resilience training can cover a broad range of topics, documented commitments by those responsible for implementing and supporting the plan are essential for the plan to be effective.

3. Revise the plan and commitments as necessary.

OTA:SG3.SP3 Establish Training Capability

A capability for delivering training to resilience staff is established and maintained.

The organization must be capable of providing resilience training across a broad range of topics and to a vast audience of resilience staff. The training must cover the topic areas of security, business continuity, and IT operations and service delivery, as well as the supporting process areas established by the operational resilience management system, including compliance management, financial resource management, and relationships with external entities, to name a few.

Capabilities for implementing the training plan must be established and maintained, including the selection of appropriate training approaches, sourcing or developing training materials, obtaining appropriate instructors, announcing the training schedule, and revising the awareness capability as needed.

If training needs have been identified for people who are not part of the organization—for example, external entities such as outsourcer, vendor, or supplier staff—then this practice should also be extensible to establish and maintain the capability to train those people as well.

Guidelines on incorporating training requirements into external entity agreements or for making organizational training assets available for use by external entities are included in the External Dependencies Management process area.

Typical work products

1. Resilience training materials and supporting work products

Subpractices

1. Select the appropriate approaches to satisfy specific organizational training needs and competencies.

   Many factors may affect the selection of training approaches, such as audience-specific knowledge, costs and schedule, and work environment. Selection of an

approach requires consideration of the means to provide skills and knowledge in the most effective way possible given the constraints.

These are examples of training approaches:

- classroom training
- computer-aided instruction
- guided self-study
- formal apprenticeship and mentoring programs
- facilitated videos
- chalk talks
- brown-bag lunch seminars
- structured on-the-job training

2. Determine whether to develop training materials internally or acquire them externally.

Criteria to consider when deciding whether to develop training materials internally or to obtain the materials externally include

- cost-benefit analysis
- schedule and availability
- availability of in-house expertise
- availability and suitability of materials from external entities

3. Develop or obtain training materials.

(Refer to the External Dependencies Management process area for guidelines on establishing and maintaining relationships with external sources of training materials.) Depending on the specific content, some customized materials may contain sensitive or proprietary information, in which case suitable provisions should be included in the external entity agreement.

4. Develop or obtain qualified instructors.

To ensure that internally provided training instructors have the necessary knowledge and training skills, criteria can be defined to identify, develop, and qualify them. In the case of externally provided training, the organization's training staff can investigate how the training provider determines which instructors will deliver the training. This can also be a factor in selecting or continuing to use a specific training provider.

5. Describe the training in the organization's training curriculum.

These are examples of the information provided in the training descriptions for each course:

- topics covered in the training
- intended audience
- prerequisites and preparation for participating
- training objectives
- length of the training
- lesson plans
- completion criteria for the course
- criteria for granting training waivers

6. Revise the training materials and supporting work products as necessary.

These are examples of situations in which the training materials and supporting work products may have to be revised:

- Training needs change (e.g., when new technology associated with the training topic is available).
- An evaluation of the training identifies the need for change (e.g., evaluations of training effectiveness surveys, training program performance assessments, or instructor evaluation forms).

OTA:SG4 Conduct Training

Training necessary for staff to perform their roles effectively is provided.

The organization must perform resilience training to ensure that staff are appropriately skilled in their roles to support the operational resilience management system. Training must be delivered according to the training plans developed and must address the vast range of needs represented in the operational resilience management system. Training records are established for the purpose of tracking training activities, and the effectiveness of the training activities is evaluated.

OTA:SG4.SP1 Deliver Resilience Training

Training is delivered according to the training plan.

Resilience training is provided by the organization (or its training provider as appropriate) to fulfill the resilience training needs and training plan. The appropriate mix of training is determined based on the needs, and the staff selected to participate in the training are determined based on their current skill level.

Training delivery for the operational resilience management system is not a trivial task. The broad range of skills necessary to address and adequately perform the competencies required to manage operational resilience requires extensive training. In addition, the intensity of the training may range from informal activities to hands-on, skill-based training.

Typical work products

1. Delivered training courses
2. Training schedule

Subpractices

1. Select the staff who will receive the training necessary to perform their roles effectively.

   Training is intended to impart knowledge and skills to people performing various roles within the organization. Some people already possess the knowledge and skills required to perform well in their designated roles. Training can be waived for these people, but care should be taken that training waivers are not abused.

2. Schedule the training, including any resources, as necessary (e.g., facilities and instructors).

Training should be planned and scheduled. Training is provided that has a direct bearing on the expectations of work performance. Therefore, optimal training occurs in a timely manner with regard to imminent job performance expectations. These expectations often include the following:

- training in the use of specialized tools
- training in procedures that are new to the individual who will perform them

3. Conduct the training.

   Experienced instructors should perform training. When possible, training is conducted in settings that closely resemble actual performance conditions and includes activities to simulate actual work situations. This approach includes integration of tools, methods, and procedures for competency development. Training is tied to work responsibilities so that on-the-job activities or other outside experiences will reinforce the training within a reasonable time after the training.

4. Track the delivery of training against the plan.

OTA:SG4.SP2 Establish Training Records

Records of delivered training are established and maintained.

Training records enable the organization to verify that training activities have been conducted according to plan. Training records may also be required to prove that a compliance obligation has been met or to support the retention of credentials or certification. Such records also facilitate the evaluation of training effectiveness.

Since this practice is related to the organization's resilience training, the training records may be a subset of the full organizational training records.

Refer to the Compliance process area for information about tracking training activities for compliance purposes.

Typical work products

1. Training records
2. Training waivers

Subpractices

1. Keep records of all staff (including external entities) indicating whether or not they successfully completed each training course or other approved training activity.
2. Keep records of all staff who have been waived from specific training.

   The rationale for granting a waiver should be documented, and both the manager responsible and the manager of the excepted individual should approve the waiver for organizational training.

3. Keep records of all staff who successfully complete their designated required training.
4. Make training records available to the appropriate people or processes.

Training records may be important in considering promotions or job assignments and thus should be made available to those who must make these types of decisions on a regular basis.

OTA:SG4.SP3 Assess Training Effectiveness

The effectiveness of the training program is assessed and corrective actions are identified.

A process should exist to determine the effectiveness of training for meeting the training needs of staff involved in the operational resilience management system.

These are examples of methods used to assess training effectiveness:

- testing in the training context
- post-training surveys of training participants
- surveys of managers' satisfaction with post-training effects
- assessment mechanisms embedded in training materials

Typical work products

1. Training effectiveness surveys
2. Instructor evaluation forms
3. Examination results or results from assessment mechanisms

Subpractices

1. Provide a mechanism for assessing the effectiveness of each training course with respect to established organizational, project, or individual learning (or performance) objectives.
2. Collect other data that can be used to evaluate training effectiveness.

   Data can be gathered through surveys or other mechanisms from course participants or from their managers to determine the impact of the training on course participants' ability to perform their resilience roles and responsibilities.
3. Document suggested improvements to the training plan based on the evaluation of the effectiveness of training activities.

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 Organizational Training and Awareness process area.

OTA:GG1 Achieve Specific Goals

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

OTA:GG1.GP1 Perform Specific Practices

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

Elaboration:

Specific practices OTA:SG1.SP1 through OTA:SG4.SP3 are performed to achieve the goals of the organizational training and awareness process.

OTA:GG2 Institutionalize a Managed Process

Organizational training and awareness is institutionalized as a managed process.

OTA:GG2.GP1 Establish Process Governance

Establish and maintain governance over the planning and performance of the organizational training and awareness process.

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

Subpractices

1. Establish governance over process activities.

   Elaboration:

   Governance over the organizational training and awareness process may be exhibited by

   - establishing a higher level position, often the director of human resources, responsible for resilience awareness, training, and staff skill and knowledge development (This role may be assisted by the operational resilience process group [ORPG].)
   - developing and publicizing higher level managers' objectives and requirements for resilience training and awareness
   - sponsoring and guiding the development of training and awareness plans that meet the organization's needs for managing operational resilience
   - sponsoring the development and implementation of training and awareness programs
   - sponsoring and funding process activities
   - sponsoring and providing oversight of policy, procedures, standards, and guidelines for training and awareness activities and programs and for organizational use of these activities and programs
   - guiding and supporting the enforcement of training and awareness requirements

- providing input on content for training and awareness programs, courses, and plans relative to organizational strategic objectives, risk appetite and tolerance, and current organizational health and condition
- making higher level-managers aware of applicable compliance obligations related to resilience training and awareness, and regularly reporting on the organization's satisfaction of these obligations to higher level managers
- verifying that the process supports strategic resilience objectives and is focused on the assets and services that are of the highest relative value in meeting strategic objectives
- regular reporting from organizational units to higher level managers on training and awareness activities and results
- creating dedicated higher level management feedback loops on decisions about the process and recommendations for improving the process
- conducting regular internal and external audits and related reporting to audit committees on process effectiveness
- creating formal programs to measure the effectiveness of process activities, and reporting these measurements to higher level managers

2. Develop and publish organizational policy for the process.

Elaboration:

The organizational training and awareness policy should address

- identifying resilience training and awareness needs
- responsibility, authority, and ownership for performing resilience training and awareness process activities, including programs and courses
- developing resilience training and awareness plans
- required participation in process activities as a condition of ongoing employment as related to resilience roles and responsibilities
- procedures, standards, and guidelines for
  - developing training and awareness attendance requirements
  - creating, delivering, and maintaining training materials
  - creating, managing, and maintaining training records
  - assessing the effectiveness of training and awareness programs
- methods for measuring adherence to policy, exceptions granted, and policy violations

OTA:GG2.GP2 Plan the Process

Establish and maintain the plan for performing the organizational training and awareness process.

Elaboration:

Specific practices OTA:SG1.SP2 and OTA:SG3.SP2 require the development of plans for how the organization will carry out organizational resilience awareness and training, respectively. In generic practice OTA:GG2.GP2, the planning elements required in specific practices OTA:SG1.SP2 and OTA:SG3.SP2 are formalized and structured and performed in a managed way. These are separate and distinct from the organizational training and awareness process plan.

Subpractices

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

   Elaboration:

   Special consideration in the plan may have to be given to training and awareness for skill development, sustaining skill competencies, and reassignment planning for various roles. These activities aid in protecting and sustaining people to support operational resilience.

   Special consideration in the plan may also have to be given to how the organization incorporates training and awareness activities for resources that are not under its direct control, including external entities such as contractors, outsourcing partners, training suppliers, and other business partners.

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

OTA:GG2.GP3 Provide Resources

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

Elaboration:

Specific practices OTA:SG1.SP2 and OTA:SG3.SP2 require the assignment of resources to the organizational resilience awareness and training plans, respectively. In generic practice OTA:GG2.GP3, resources are formally identified and assigned to plan elements. These are separate and distinct from the resources required to execute the organizational training and awareness process plan.

The diversity of activities required to ensure adequate, up-to-date training and awareness of resilience staff requires an extensive level of organizational resources and skills and may require a significant number of external resources. In addition, these activities may require a major commitment of financial resources (both expense and capital) from the organization.

Subpractices

1. Staff the process.

   Elaboration:

   This generic goal related to organizational training and awareness refers to staffing the organizational training and awareness process plan, not the individual organizational training and awareness plans. Assigning resources to organizational training and awareness plans is included in specific practices OTA:SG1.SP2 and OTA:SG3.SP2.

   These are examples of staff required to perform the organizational training and awareness process:

   - subject matter experts, including staff knowledgeable of each operational resilience management process area and how to reflect process requirements in awareness and training materials
   - curriculum designers

- instructional designers
- instructors
- training administrators
- human resources staff
- staff responsible for developing training and awareness plans and programs and ensuring they are aligned with stakeholder requirements and needs
- external entities involved in creating, delivering, and maintaining training and awareness materials
- staff responsible for managing external entities that have contractual obligations for resilience training and awareness activities
- internal and external auditors responsible for reporting to appropriate committees on process effectiveness

Refer to the Human Resource Management process area for information about acquiring staff for resilience roles and responsibilities.

2. Fund the process.

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

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

   Elaboration:

   These are examples of tools, techniques, and methods to support the organizational training and awareness process:

   - methods and tools for building and distributing awareness messages, including pens, mugs, posters, signage, screen savers, newsletters, etc. (as described in OTA:SG1.SP3 subpractice 1)
   - instruments for analyzing training needs
   - training workstations and other hardware needs
   - instructional design tools
   - packages for developing presentation materials
   - tools, methods, and procedures that closely resemble actual performance conditions and simulate actual work situations
   - methods for delivering awareness and training materials, from user on-demand training to classroom-based training
   - tools for tracking awareness and training course attendance and successful and unsuccessful completion by designated staff
   - methods for evaluating the effectiveness of awareness activities, including surveys, focus groups, interviews, etc. (as described in OTA:SG2.SP3)
   - methods for evaluating the effectiveness of training activities, including testing, assessment mechanisms, etc. (as described in OTA:SG4.SP3)
   - tools used to capture and securely store training records and ensure such records are accessed only by authorized staff

OTA:GG2.GP4 Assign Responsibility

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

Elaboration:

Specific practices OTA:SG1.SP2 and OTA:SG3.SP2 require the assignment of responsibility to the organizational awareness and training plans. In generic practice OTA:GG2.GP4, commitments are formally identified to support resource allocations to plan elements. These are separate and distinct from the assignment of responsibilities for the organizational training and awareness process plan.

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

Subpractices

1. Assign responsibility and authority for performing the process.

   Elaboration:

   Responsibility and authority may extend not only to staff inside the organization but to those external entities with which the organization has a contractual agreement for creating, delivering, and maintaining awareness and training materials.

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

   Elaboration:

   Responsibility and authority for performing organizational training and awareness tasks can be formalized by

   - defining roles and responsibilities in the process plan
   - 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 to participate in and derive benefit from the process for services and assets under their ownership or custodianship
   - developing policy requiring participation in process activities as a condition of ongoing employment
   - including process tasks in staff performance management goals and objectives, with requisite measurement of progress against these goals
   - developing and implementing contractual instruments (as well as service level agreements) with external entities to establish responsibility and authority for creating, delivering, and maintaining awareness and training materials, where applicable
   - including process tasks in measuring performance of external entities against service level agreements

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.

OTA:GG2.GP5 Train People

Train the people performing or supporting the organizational training and awareness process as needed.

Elaboration:

Specific practices OTA:SG1.SP1 and OTA:SG3.SP1 call for establishing awareness needs and training needs for resilience awareness and training plans and programs, respectively.

Refer to the External Dependencies Management process area for more information about awareness training for external entities such as business partners, suppliers, and vendors.

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 skill needs are related to delivering the organizational training and awareness process, not the development and delivery of subject matter information related to security, business continuity, IT operations management, or the management of operational resilience. The identification of skill needs for subject matter areas is included in the subpractices for generic practice GG2.GP5 in each of the individual process areas.

   These are examples of skills required in the organizational training and awareness process:

   - curriculum and instructional design
   - course delivery
   - course and instructor evaluation
   - measuring the effectiveness of awareness and training materials
   - structuring and conducting participant surveys and interviews
   - knowledge of the tools, techniques, and methods necessary to create, deliver, and maintain training and awareness work products, including those necessary to perform the process using the selected methods, techniques, and tools identified in OTA:GG2.GP3 subpractice 3
   - knowledge unique to each operational resilience management process area and assets and services that are the focus of these processes
   - knowledge necessary to elicit and prioritize stakeholder requirements and needs and interpret them to develop effective process requirements, plans, and programs

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:
   - knowledge and skills needs analysis
   - instructional design
   - instructional techniques
   - refresher training on subject matter
   - supporting resilience staff in understanding the process and their roles and responsibilities with respect to its activities
   - working with external entities that have responsibility for resilience training and awareness activities
   - using process methods, tools, and techniques, including those identified in OTA:GG2:GP3 subpractice 3
4. Provide training and review the training needs as necessary.

OTA:GG2.GP6 Control Work Products

Place designated work products of the organizational training and awareness process under appropriate levels of control.

Refer to the Compliance process area for information about tracking of awareness activities for compliance purposes.

Elaboration:

Specific practices OTA:SG2.SP2 and OTA:SG4.SP2 address the record keeping and documentation process over organizational training and awareness activities.

These are examples of organizational training and awareness work products placed under control:
- awareness and training needs
- awareness and training plans and programs
- awareness and training records and waivers
- awareness and training materials and supporting work products
- instructor evaluation forms
- awareness and training effectiveness surveys
- survey and interview results
- awareness and training examinations and assessment results
- policies and procedures
- contracts with external entities

OTA:GG2.GP7 Identify and Involve Relevant Stakeholders

Identify and involve the relevant stakeholders of the organizational training and awareness process as planned.

Elaboration:

Many OTA-specific practices address the involvement of stakeholders in the organizational training and awareness process. For example, specific practice OTA:SG1.SP1 calls for identifying staff groups and their particular awareness needs. Specific practice OTA:SG1.SP2 ensures these needs are carried out in the awareness training plan.

Subpractices

1. Identify process stakeholders and their appropriate involvement.

   Elaboration:

   These are examples of stakeholders of the organizational training and awareness process:

   - staff who are required to determine the degree to which their constituencies understand the organization's resilience goals, objectives, standards, policies, and processes, including
     - asset owners and custodians
     - service owners
     - business process owners
     - organizational unit and line of business managers responsible for high-value services and assets
   - external entities responsible for managing high-value assets and services
   - human resources (for ensuring the resilience of people assets)
   - information technology staff (for ensuring the resilience of technology assets)
   - staff responsible for physical security (for ensuring the resilience of facility assets)
   - internal and external auditors

   Stakeholders are involved in various tasks in the organizational training and awareness process, such as

   - planning for the process
   - making decisions about the process
   - making commitments to process plans and activities
   - communicating process plans and activities
   - coordinating process activities
   - reviewing and appraising the effectiveness of process activities
   - establishing requirements for the process
   - resolving issues in the process

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

OTA:GG2.GP8 Measure and Control the Process

Measure and control the organizational training and awareness process against the plan for performing the process and take appropriate corrective action.

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

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

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

Subpractices

1. Measure actual performance against the plan for performing the process.
2. Review accomplishments and results of the process against the plan for performing the process.

   Elaboration:

   These are examples of metrics for the organizational training and awareness process:

   - percentage of awareness needs for each staff group that are addressed in the awareness plan
   - difference in planned versus actual awareness sessions delivered
   - schedule of delivery of awareness sessions (planned frequency versus actual frequency)
   - elapsed time since awareness materials were reviewed and updated
   - percentage of new users (internal and external) who have satisfactorily completed awareness sessions before being granted network access
   - percentage of users (internal and external) who have satisfactorily completed periodic awareness refresher sessions as required by policy
   - percentage of awareness activities that include a mechanism for evaluating the effectiveness of the awareness activity
   - percentage of passing scores (by participants) on awareness assessments
   - percentage of staff who have been assessed to determine if their level of awareness is commensurate with their job responsibilities
   - percentage of staff waived from awareness activities
   - percentage of training needs for each role and responsibility that are addressed in the training plan
   - difference in planned versus actual training courses delivered
   - schedule of delivery of training sessions (planned frequency versus actual frequency)
   - percentage of favorable post-training evaluation ratings, including instructor ratings
   - elapsed time since training materials were reviewed and updated

- number of internal staff members for whom training was planned versus number trained (percentage)
- number of external staff members for whom training was expected or contracted versus number trained (percentage)
- percentage of favorable training program quality survey ratings
- percentage of passing scores (by participants) on training examinations
- percentage of staff who have been assessed to determine if training has been effective commensurate with their job responsibilities
- percentage of staff waived from training

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 organizational training and awareness process are needed to ensure that

   - training and awareness plans and programs are developed and implemented
   - training and awareness needs have been identified and are being satisfied
   - training and awareness activities are conducted as scheduled
   - all staff regularly attend training and awareness events as required by their roles and responsibilities
   - the waiver process is not abused
   - training and awareness activities are recorded
   - skills necessary to develop and deliver training and awareness programs are available or obtainable
   - the performance and effectiveness of training and awareness programs are regularly monitored, reported, evaluated, and improved
   - training and awareness materials are regularly reviewed and updated as required
   - training and awareness issues are referred to the risk management process when necessary
   - actions requiring management involvement are elevated in a timely manner
   - key measures are within acceptable ranges as demonstrated in governance dashboards or scorecards and financial reports
   - 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.

   Elaboration:

   Deviations from the organizational training and awareness plan may occur when organizational units fail to follow the enterprise-sponsored process. These deviations may affect the operational resilience of the organizational unit's services but may also have a cascading effect on enterprise operational resilience objectives.

5. Identify problems in the plan for performing and executing the process.

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

OTA:GG2.GP9 Objectively Evaluate Adherence

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

Elaboration:

These are examples of activities to be reviewed:

- the identification of training and awareness needs and the development of plans and programs to meet these needs
- regular offering of and attendance at training and awareness activities
- the alignment of stakeholder requirements with process plans and programs
- assignment of responsibility, accountability, and authority for process activities
- determination of the adequacy of process reports and reviews in informing decision makers regarding the performance of operational resilience management activities and the need to take corrective action, if any
- use of process work products for improving strategies to protect and sustain assets and services

These are examples of work products to be reviewed:

- tactical plans for training and awareness
- awareness and training materials and supporting work products
- awareness and training records, including waivers
- instructor, awareness session, and training evaluation forms
- surveys
- process plan and policies
- issues that have been referred to the risk management process
- process methods, techniques, and tools
- contracts with external entities
- metrics for the process (Refer to OTA:GG2.GP8 subpractice 2.)

OTA:GG2.GP10 Review Status with Higher Level Managers

Review the activities, status, and results of the organizational training and awareness 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.

OTA:GG3 Institutionalize a Defined Process

Organizational training and awareness is institutionalized as a defined process.

OTA:GG3.GP1 Establish a Defined Process

Establish and maintain the description of a defined organizational training and awareness 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 organizational training and awareness process and best meet the needs of the organizational unit or line of business.

   Elaboration:

   Each organizational unit will perform organizational training and awareness in a slightly different manner depending on operational concerns, identified needs and skill gaps, availability of supporting infrastructure, and requirements.

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.

OTA:GG3.GP2 Collect Improvement Information

Collect organizational training and awareness work products, measures, measurement results, and improvement information derived from planning and performing the process to support future use and improvement of the organization's processes and process assets.

Elaboration:

These are examples of improvement work products and information:

- results of training effectiveness surveys
- training program performance assessment results
- course evaluations
- training records
- training requirements from a stakeholder group

- proper and improper use of awareness and training waivers
- reports on the weaknesses of controls that can be addressed in training and awareness activities
- changes and trends in operating conditions, risk conditions, and the risk environment that affect process offerings
- lessons learned in post-event review of incidents and disruptions in continuity, including lack of staff preparedness to fulfill roles and responsibilities
- 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.