CRR Supplemental Resource Guide

Volume 9

Training and Awareness

Version 1.1

This material is based upon work funded and supported by Department of Homeland Security 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-0003284

Table of Contents

I. Introduction

Series Welcome

Welcome to the CRR Supplemental Resource Guide series! This document was developed by the Department of Homeland Security's (DHS) Cyber Security Evaluation Program (CSEP). It is the ninth of 10 resource guides intended to help organizations implement practices identified as considerations for improvement during a Cyber Resilience Review (CRR).[1] The CRR is an interview-based assessment that captures an understanding and qualitative measurement of an organization's *operational resilience* for IT operations. Operational resilience indicates the organization's ability to adapt to risk that affects its core operational capacities.[2] It also highlights the organization's ability to manage operational risks to critical services and associated assets during normal operations as well as times of operational stress and crisis. The guides were developed for organizations that have participated in a CRR, but are useful to any organization interested in implementing or maturing operational resilience capabilities for critical IT services.

The 10 domains covered by the CRR Resource Guide series are

1. Asset Management
2. Controls Management
3. Configuration and Change Management
4. Vulnerability Management
5. Incident Management
6. Service Continuity Management
7. Risk Management
8. External Dependencies Management
9. **Training and Awareness** ⇦***This guide***
10. Situational Awareness

The objective of the CRR is to allow organizations to measure the performance of fundamental cyber security practices. DHS introduced the CRR in 2011. In 2014 DHS launched the Critical Infrastructure Cyber Community or C³ (pronounced "C Cubed") Voluntary Program to assist the enhancement of critical infrastructure cybersecurity and to encourage the adoption of the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF). The NIST CSF provides a common taxonomy and mechanism for organizations to

1. describe their current cybersecurity posture
2. describe their target state for cybersecurity
3. identify and prioritize opportunities for improvement within the context of a continuous and repeatable process
4. assess progress toward the target state

5. communicate among internal and external stakeholders about cybersecurity risk

The CRR Self-Assessment Package includes a correlation of the practices measured in the CRR to criteria of the NIST CSF. An organization can use the output of the CRR to approximate its conformance with the NIST CSF. It is important to note that the CRR and NIST CSF are based on different catalogs of practice. As a result, an organization's fulfillment of CRR practices and capabilities may fall short of, or exceed, corresponding practices and capabilities in the NIST CSF.

Each resource guide in this series has the same basic structure but can be used independently. Each guide focuses on the development of plans and artifacts that support the implementation and execution of operational resilience capabilities. Organizations using more than one resource guide will be able to make use of complementary materials and suggestions to optimize their adoption approach. Stakeholders identified in the implementation of other domains may also be stakeholders in training and awareness. Training and awareness can be used to support and reinforce the implementation of the other nine domains. For example, in incident management, training provides the incident response team with the understanding of how the team works together to respond to incidents; in controls management, awareness activities inform staff of newly deployed controls such as new password requirements.

Each guide derives its information from best practices described in a number of sources, but primarily from the CERT®-Resilience Management Model (CERT®-RMM).[3] The CERT-RMM is a maturity model for managing and improving operational resilience, developed by the CERT Division of Carnegie Mellon University's Software Engineering Institute (SEI). This model is meant to

- guide the implementation and management of operational resilience activities
- converge key operational risk management activities
- define maturity through capability levels
- enable maturity measurement against the model
- improve an organization's confidence in its response to operational stress and crisis

The CERT-RMM provides the framework from which the CRR is derived—in other words, the CRR method bases its goals and practices on the CERT-RMM process areas.

This guide is intended for organizations seeking help in establishing a training and awareness process. To outline this process, this document will use an approach common to many organizations. The process phases described include

- create a training and awareness plan
- assess training and awareness needs
- conduct training and awareness activities
- improve training and awareness capability

More specifically this guide

- educates and informs readers about the training and awareness process
- promotes a common understanding of the need for a training and awareness process
- identifies and describes key practices for training and awareness
- provides examples and guidance to organizations wishing to implement these practices

® CERT® is a registered mark owned by Carnegie Mellon University.

Additionally, Appendix B provides a mapping between the practices that constitute the Training and Awareness domain in the CRR and the appropriate Function, Category, and Subcategory in the NIST CSF.

The guide is structured as follows:

I. Introduction—Introduces the *CRR Resource Guide* series and describes the content and structure of these documents.

II. Training and Awareness—Presents an overview of the training and awareness process and establishes some basic terminology.

III. Plan for Training and Awareness—Highlights the elements necessary for an effective training and awareness plan.

IV. Assess Training and Awareness Needs—Presents an approach for identifying cybersecurity-related skills needed for specific roles (administrators, technicians, etc.) and cybersecurity awareness needs for staff throughout the organization.

V. Conduct Training and Awareness Activities—Outlines a process that defines the steps necessary to manage, develop, schedule, and conduct training and awareness activities.

VI. Improve Training and Awareness Capability—Provides an approach for evaluating and improving training and awareness capability.

VII. Conclusion—Highlights the key points from this guide and provides contacts and references for further information.

Appendices

A. Training and Awareness Resources
B. CRR/CERT-RMM Practice/NIST CSF Subcategory Reference

Audience

The principal audience for this guide includes individuals responsible for designing, managing, or conducting training and awareness. Executives who establish policies and priorities for training and awareness, managers and planners who are responsible for converting executive decisions into plans, and staff responsible for implementing the plans and conducting training and awareness activities can also benefit from this guide.

To learn more about the source documents for this guide and for other documents of interest, see Appendix A.

II. Training and Awareness

Overview

Training and awareness focuses on the processes by which an organization plans, identifies needs for, conducts, and improves training and awareness to ensure the organization's operational cyber resilience requirements and goals are known and used. The process depicted in Figure 1 helps the organization ensure that the training and awareness process supports the organization's cyber resilience objectives. This guide focuses on the training and awareness activities that make staff members aware of their role in the organization's cyber resilience concerns and policies. Staff members also receive specific training to enable them to perform their roles in managing organizational cyber resilience. Though this guide focuses on training and awareness for cyber resilience activities, these activities should integrate with and support the organization's overall training and awareness program. If the organization already has training or awareness programs, it is important that they include cyber resilience. Existing programs can use their established information gathering processes, building capabilities, evaluation methods, record keeping, and improvement activities to support cyber resilience training and awareness.

The training and awareness domain focuses on general awareness, skill building, and ongoing training.[4]

Figure 1: The Training and Awareness Process

In this guide, *training* refers to a set of activities that focuses on staff members learning the skills and gaining the knowledge needed to perform their roles and responsibilities in support of their organization's resilience program. Awareness activities focus on staff members developing an understanding of resilience issues, concerns, policies, plans, and practices. The high-level outline below highlights the main areas of this domain and points the reader to the corresponding details in this guide.

The following sections detail each of the steps in the training and awareness process.

Training and Awareness Process

Plan for Training and Awareness

Training and awareness is a support process that ensures staff members have the knowledge and skills to perform their work, including work in other processes such as incident management, controls management, and risk management. Training and awareness typically takes place at various levels of an organization. Enterprise training and awareness addresses organization-wide needs. Specific training and awareness activities are typically developed and implemented at the organizational level (e.g., business unit or team) where they are needed. For training and awareness at any level of the organization, management support is essential. With management support, processes are defined to identify, implement, and assess training and awareness on an ongoing basis to ensure skilled employees can provide resilient services.

Planning for training and awareness is essential for a successful program. The plan documents the program objectives, strategy for achieving those objectives, and the infrastructure and resources needed to execute the plan.

Important activities while planning for training and awareness include the following:

- Obtain support for training and awareness planning.
- Establish a training and awareness program strategy.
- Establish an approach to building a training capability.
- Establish an approach to building an awareness capability.

Assess Training and Awareness Needs

The identification of training and awareness needs provides critical information for the development of a training and awareness program. If the organization has an established training and awareness program, there may already be a needs analysis process in place. Still, the organization should review the previously identified needs to ensure they include those specific to cyber resilience and, periodically, to see if any of the needs have changed.

Training and awareness needs specific to cyber resilience can be derived from other domain plans (e.g., controls management and risk management). Those plans include a list of critical skills needed to perform the planned work. Job descriptions also provide information on skills and knowledge needed to perform a particular job. As the organization assigns roles to staff, it should identify any gaps in skills and knowledge as training needs. It should also review domain plans to identify the activities needed to educate staff members about the organization's cyber resilience concerns, which inform the organization's awareness needs. Once training and awareness needs are identified, an organization must analyze those needs to determine what actions it will take to resolve the gaps.

Important activities for identifying training and awareness needs include the following:

- Obtain support for training and awareness needs assessment.
- Establish a strategy for identifying training needs.
- Establish a strategy for identifying awareness needs.
- Establish a process for training and awareness needs analysis.

Training needs are the documented gaps between current skills of people assigned to roles and the skills they need to effectively perform the role's work. Awareness needs are the communications capabilities that an organization needs to inform staff of cyber resilience concerns.

Conduct Training and Awareness Activities

Building capability and conducting training and awareness activities usually involve engaging multiple levels of the organization as well as third-party providers. Cyber resilience efforts should be incorporated into any existing training and awareness program and evaluated for effectiveness. Establishing capability for cyber resilience training and awareness includes identifying and developing the program's educational vehicles (courses, presentations, etc.). Each organization will have unique needs for cyber resilience training and awareness that must be addressed with activities developed specifically for the organization, as well as common needs that can be met by third-party providers.

Important activities for building capability and conducting training and awareness include the following:

- Establish and maintain support functions for training and awareness (e.g., library for storing materials and a record tracking system).
- Develop training and awareness materials.
- Procure third-party provider services.
- Conduct training and awareness activities.

Improve Training and Awareness Capability

In the evaluation and improvement phase of the training and awareness process, the organization should evaluate existing training and awareness activities against the organization's objectives. If the activities are not meeting their objectives, then the organization must initiate improvement actions. Improvements to the training and awareness activities, based on the analysis of the collected data, should support the achievement of organizational objectives.

To be effective, training and awareness activities must be meaningful to both the employee and the organization. Evaluators must plan ahead to collect sufficient data to examine the effectiveness of the activities and recommend improvements to be incorporated in the next cycle. The data collected should allow the analysis of the programs against four desired outcomes:

- Employees are better able to perform their jobs.
- Supervisors are better able to assess changes to their employees' on-the-job performance.
- The organization feels confident that the employees are performing activities in a way that demonstrates a resilient organization (e.g., meets the goals and objectives).
- The training and awareness activities can be improved.

Evaluation requires the collection of data and observations throughout the organization's training cycle. Evaluation and analysis of training and awareness programs should occur at an organizationally defined

frequency to support the incorporation of updated material and synchronization with the execution of the training and awareness plan.

Important activities in the training and awareness assessment process include the following:

- Establish a plan to evaluate the training and awareness program.
- Evaluate the training and awareness program and analyze results.
- Improve the process.
- Update training and awareness materials.

Summary of Steps

The following sections of this guide lay out the discrete steps for developing a plan to implement the training and awareness process as described above:

Plan for Training and Awareness

1. Obtain support for training and awareness planning.
2. Establish a training and awareness program strategy.
3. Establish an approach to building a training capability.
4. Establish an approach to building an awareness capability.

Assess Training and Awareness Needs

1. Obtain support for training and awareness needs assessment.
2. Establish a strategy for identifying training needs.
3. Establish a strategy for identifying awareness needs.
4. Establish a process for training and awareness needs analysis.

Conduct Training and Awareness Activities

1. Establish and maintain support functions for training and awareness.
2. Develop training and awareness materials.
3. Procure third-party provider services.
4. Conduct training and awareness activities.

Improve Training and Awareness Capability

1. Establish a plan to evaluate the training and awareness program.
2. Evaluate the training and awareness program and analyze results.
3. Improve the process.
4. Update training and awareness materials.

Organizations that already have a training and awareness program can assess and improve it by using the guidance in this resource guide.

III. Plan for Training and Awareness

Before You Begin

The following checklist summarizes the tasks you will need to complete and the information you will need to gather before you can begin developing a training and awareness program.

	Input	Guidance
✓	Scoping statement	This statement defines what the training and awareness program and plan need to address. Training and awareness should cover, at a minimum, all critical organizational services. Organizations that are not sure where to start should focus on the most essential services and the areas that directly affect their mission. This approach may allow an organization to address the areas of greatest risk first and mitigate their impact while training and awareness objectives are being defined for noncritical areas. If your organization has participated in a CRR, it may be beneficial to begin with the critical service addressed during the CRR. See Appendix B for a cross-reference between the CRR and this guide.
✓	List of stakeholders	The list of stakeholders should be aligned to the scoping statement and include all appropriate internal and external entities. Potential candidates include • executive and senior management • heads of business lines, especially critical services owners • information technology • legal • human resources • third-party providers (e.g., training vendors) • training and awareness program staff • compliance personnel
✓	Management support	Sponsorship by senior management is necessary for establishing a training and awareness program and implementing processes. This should include the appropriate funding and resources to implement the activities described in this guide as well as support and oversight to ensure that these activities are aligned with the other activities in the organization.
✓	An understanding and acknowledgement of an acceptable approach to training and awareness	Acknowledgement from management for the intended approach to training and awareness, including stakeholder expectations about acceptable risk tolerance for the identified critical assets and services, is required.
✓	Externally imposed requirements for training and awareness	Regulatory requirements define mandatory training and awareness, certifications, qualifications, and other needs (this includes service-level agreement requirements).
✓	List of critical services	To properly develop a training and awareness program, the critical services in the organization need to be identified.
✓	Risks	Obtain the list of categorized and prioritized risks. Risks change over time, so it is important that the updated list is provided when risks change.
✓	Assignment of responsibility for training and awareness	Job descriptions for roles that have responsibilities for training and awareness should reflect those responsibilities (for example, executive ownership, planning, development of training and awareness capability, and delivery of training and awareness).

	Input	Guidance
✓	Budget for training and awareness	Identify the available funds to perform training and awareness planning and execution, including • staffing resources • tools (applications and associated hardware) • third-party support

Step 1. Obtain support for training and awareness planning.

Obtaining support from management is essential to ensuring the training and awareness plan is effectively implemented. A top-down approach is often helpful in ensuring the training and awareness program meets the resilience objectives of the organization.

The level of management support required depends on the scope of the training and awareness program being implemented. Senior-executive-level support is necessary for a training and awareness plan that addresses the entire organization. Smaller implementations, such as those at the service level, may require sponsorship only from management responsible for that particular service. To illustrate, consider an electric utility company that has four main services: generation, transmission, distribution, and business support. A training and awareness program could be implemented for these services individually. When the scope is limited to a single service or component of an organization, the involvement and support of the organization's senior management may be limited, and more involvement might be required from management within the individual service or component.

Initially, training and awareness planning is usually iterative. As the other phases of the training and awareness process are completed (needs assessment, conducting training and awareness, and improvement), the plan will need to be reviewed and revised. Eventually, training and awareness planning might be done more periodically.

Step 2. Establish a training and awareness program strategy.

A training and awareness program should be developed to reflect priorities at the enterprise and operating-unit levels as well as for specific critical services. The following steps illustrate an approach for establishing objectives for a training and awareness program:

A. Identify management directives and organizational priorities. Organizational priorities can be articulated in many forms and help identify the strategic objectives. Strategic objectives are derived from strategic planning activities, which usually forecast two to five years out.[5] The following sources can provide insight into management directives and organizational guidelines:

- strategic plan—The document in which an organization defines its plans for achieving its mission, where the organization wants to go, and how it plans on getting there.[6] Large enterprises may have strategic plans at multiple levels within the organization, such as the enterprise and operating-unit levels.
- critical success factors (CSFs)—A small number of areas in which an organization must consistently perform well to meet its goals and mission.[7] CSFs illustrate what the organization considers its top priorities in achieving its goals.

- legal and regulatory obligations—Obligations that often give insight into requirements placed on the organization by external entities.[8]
- internal policies and standards—Policies and procedures developed by the organization to promote acceptable behaviors and practices.[9]

B. Define and document training and awareness program objectives. Training and awareness program objectives are derived from the management directives and organizational priorities identified above.

C. Prioritize training and awareness program objectives. Training and awareness program objectives should be prioritized based on their potential to affect operational resilience.[10] This will help the organization determine the allocation of resources, such as the number of staff members requiring training and types of training and awareness activities (e.g., in-house or vendor-supplied).

The resources available to an organization for training and awareness will influence the strategy selection. The training and awareness program strategy should

- focus on increasing the cyber resilience of critical services
- align with the organization's strategic objectives

The purpose of a training and awareness program is to identify specific activities that can implement and support the training and awareness objectives.

The following steps illustrate an approach for integrating training and awareness objectives specific to cyber resilience in an existing training and awareness program:

A. Review the existing activities before implementing new training and awareness program activities. This will ensure new training and awareness activities are not redundant.

B. Review existing training and awareness program activities to determine if they are still effective. This review is often completed as a by-product of auditing or feedback and measurement activities. A training and awareness program activities assessment should provide sufficient evidence to determine the effectiveness of the implemented training and awareness program activities.

C. Establish new training and awareness program activities to fill the gaps between existing activities and needed ones. (See Section VI, Steps 2 and 3 for more information on identifying training and awareness needs.)

D. Confirm existing and updated training and awareness program activities are still relevant, and assign responsibility for implementation of new activities. Responsibility for ensuring that training and awareness program activities are implemented typically rests with the operating-unit managers.

To put training and awareness program activities into perspective, consider a large enterprise with multiple operating units consolidated onto one campus. The activities will likely be controlled by one operating unit responsible for the training and awareness program activities affecting the critical services. Because the other operating units share the facility, they can participate and benefit from the same training and awareness program activities.

Step 3. Establish an approach to building a training capability.

When establishing its approach to building a training capability, the organization needs to consider the types of training needed and how that training will be sourced. Will it be developed in-house or procured from a third-party provider? Most training programs use a combination of training options based on what best meets their training needs and are guided by the training strategy and objectives.

"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." CERT-RMM, p. 666

There are many different training approaches, including the following examples:

- classroom training
- guided self-study
- on-the-job training
- mentoring programs
- online training
- webinars and podcasts

Determining which approach to use depends on factors such as needed skills and knowledge, budget, audience, availability, and work environment. Classroom training provides a rich learning environment, but it is also expensive, and attendees must be available for the duration of the class. In contrast, on-the-job training provides hands-on skill development in the learner's work environment, though with the potential drawback of incomplete or inconsistent training opportunities. All of the approaches require attention to learning objectives and the training materials that support them.

Step 4. Establish an approach to building an awareness capability.

The overlap between building a training capability and an awareness capability is often minimal, so it is important to define the approaches separately.

"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." CERT-RMM, p. 658

Below is a list of example approaches:

- poster campaigns
- newsletters
- email messages
- presentations at organization-wide or team meetings
- trainer-facilitated sessions
- informal sessions (e.g., brown bag lunches, webinars, conferences)

As the training and awareness plan documentation matures, the organization needs to address a few questions about building an internal organizational infrastructure to support the implementation of the plan, presented in Table 1.

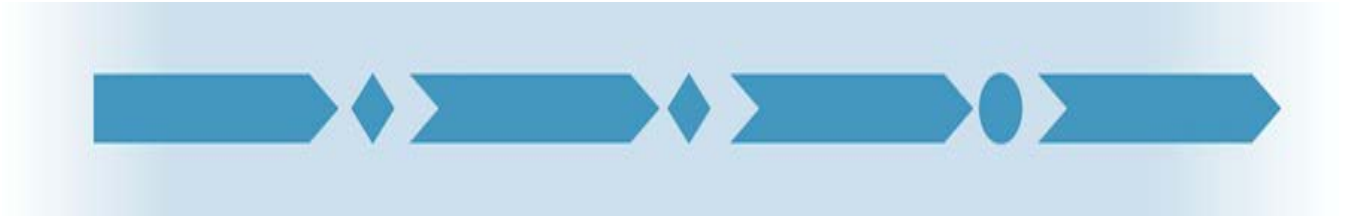
Table 1: Training and Awareness Planning Questions

Can you answer YES?	Questions
	Do we know what roles/positions we need filled now?
	Do we know what roles/positions we would like to have?
	Do we have a good account of the team's capabilities (skills, training)?
	Do we have actual job descriptions for every role we need to grow?
	Do we have training events/resources in our budget and on our calendar?
When you answer all of these as YES!—then you can feel comfortable that you have a plan.	

Once your organization has documented its training and awareness plan, standards, and guidelines, it should review and update them periodically (at least annually or as required by other guidelines) and as driven by events (e.g., critical service change, significant organizational changes) to ensure they are achieving the desired results.

Output of Section III

	Output	Guidance
✓	Management directives and guidelines	Management directives and guidelines should be clearly identified.
✓	Training and awareness program objectives	Using the management directives and guidelines, training and awareness program objectives should be defined.
✓	Training and awareness program activities strategy	Organizations should identify the appropriate mix of training and awareness program activities to achieve the program objectives.
✓	Approach to building a training capacity	Training capability that meets the training objectives is identified.
✓	Approach to building an awareness capability	Awareness capability that meets the awareness objectives is identified.
✓	Training and awareness plan	Training and awareness strategy and objectives are documented with the initial approach for implementation and identified resources needed.



IV. Assess Training and Awareness Needs

Before You Begin

The following checklist summarizes the tasks you will need to complete and the information you will need to gather before you can begin assessing training and awareness needs.

	Input	Guidance
✓	Scoping statement	This statement defines the boundaries of the training and awareness needs assessment. The assessment should cover critical organizational services. Organizations that are not sure where to start should focus on the most essential services and the areas that directly affect their mission. If your organization has participated in a CRR, it may be beneficial to begin with the critical service addressed during the CRR. See Appendix B for a cross-reference between the CRR and this guide.
✓	List of stakeholders	The list of stakeholders should be aligned to the scoping statement and include all appropriate internal and external entities. Potential candidates include • executive and senior management • heads of business lines, especially critical services owners • information technology • human resources • managers of resilience management activities (e.g., incident management, controls, situation awareness, service continuity) • managers of the critical services
✓	Management support	Senior management should provide an endorsement for conducting a training and awareness needs assessment.
✓	Assignment of responsibility for training and awareness needs assessment	Job descriptions for roles that have responsibilities for training and awareness (for example, executive ownership, human resources, training and awareness program personnel) should clearly state those responsibilities. Also, the training and awareness responsibilities of managers of critical services and managers of cyber resilience activities should be clearly defined.
✓	Budget for training and awareness needs assessment	Identify available funds to perform a training and awareness needs assessment, including • staffing resources • tools (applications and associated hardware) • third-party support, if needed

Step 1. Obtain support for training and awareness needs assessment.

Obtaining support from management is essential to ensuring that the training and awareness needs assessment is effectively conducted. The level of management support required depends on the scope of the needs assessment being conducted. When the scope is limited to a single service or component of an organization, the involvement and support of the organization's senior management may be limited, and more involvement might be required from officials within the individual service or component.

Step 2. Establish a strategy for identifying training needs.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/ Subcategory
Goal 1 – Cyber security awareness and training programs are established.	
2. Have required skills been identified for specific roles (administrators, technicians, etc.) for the critical service? [HRM:SG1.SP2]	**PR.AT-1: All users are informed and trained**
3. Are skills gaps present in personnel responsible for cyber security identified? [OTA: SG3.SP1]	**PR.AT-1: All users are informed and trained**

Training needs are derived by identifying the skills and knowledge required to perform the necessary work and comparing them to the current skills and knowledge capabilities of the assigned personnel. Any gaps that prevent personnel from effectively performing their work are identified as training needs. If the organization has an established training program, there may already be a needs analysis process in place. Still, the organization should review the previously identified needs to ensure they include those specific to cyber resilience.

If the organization does not have a training program, then it should develop an approach for data collection and analysis. There are many ways to collect the necessary data, for example, document review (e.g., domain-related plans), surveys, interviews, questionnaires, user observation, workshops, exercises, brain storming, use cases, prototypes, and role playing. Using a variety of elicitation techniques may facilitate initial needs assessments. Once the needs are established, a simple review by key stakeholders will ensure that this is still an accurate picture of the needs.

One approach to identifying training needs specific to cyber resilience is to use domain-related plans (e.g., controls management plan, risk management plan). Those plans should include a list of critical skills and knowledge needed to perform the planned work. Job descriptions also provide information on skills and knowledge needed to perform a particular job. As the organization assigns roles to staff, it should identify any gaps in skills and knowledge as training needs. If plans or skills and knowledge information are not available, it may be necessary to gather training needs through interviews with managers responsible for the different aspects of the organization's cyber resilience efforts or from employee training and development plans.

Training needs are documented and accumulated across the organization, providing an overall picture of the number of people who need training in different skill and knowledge categories. This information is used in the analysis step (Section IV, Step 4).

Step 3. Establish a strategy for identifying awareness needs.

Unlike skills training, awareness efforts communicate a message to a broad group of employees with different skills and experience. The awareness message often conveys information about organizational goals, objectives, and critical success factors. The message can also provide employees with information that improves operational resilience (e.g., security and confidentiality guidelines, vulnerability and incident notices). Awareness needs are identified through multiple sources, such as

- resilience requirements
- organizational policies
- vulnerabilities under watch
- laws and regulations

- service continuity plans

In addition, plans for domain processes can be reviewed for awareness activities needed to provide staff members with an understanding of the organization's cyber resilience concerns. Another way to gather awareness needs information is to interview managers responsible for the different aspects of the organization's cyber resilience efforts.

It is also useful to identify different groups of people by the types of awareness information they need. For example, the general population of an organization may need information about organizational goals and objectives, and those responsible for responding to a service disruption will need information on changes to service continuity plans.

Documenting and accumulating awareness needs across the organization provides an overall picture of the extent of awareness activities to be conducted, as well as the different awareness categories (such as personnel groups or need for urgency). This information is used in the analysis step (Section IV, Step 4).

Step 4. Establish a process for training and awareness needs analysis.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/ Subcategory
Goal 1 – Cyber security awareness and training programs are established.	
1. Have cyber security awareness needs been identified for the critical service? [OTA:SG1.SP1]	**PR.AT-1: All users are informed and trained**
4. Have training needs been identified? [OTA: SG3.SP1]	**PR.AT-1: All users are informed and trained**

The organization must analyze its training and awareness needs to determine how it will resolve the gaps and meet organizational goals. Table 2 and Table 3 outline an approach to analyzing training and awareness needs.

Table 2: Training Needs Analysis

Activity	Details
Compare required skills and knowledge and current skills and knowledge to identify gaps (training needs).	Review the identified training needs to determine if the program can meet them.
Categorize the training needs.	Example categories include • technical skills • process knowledge and skills • resilience knowledge
Create a table showing training needs by category and number of people needing the training.	Gain a better understanding of the extent of the training need across categories and the actual number of people needing the training.
Determine if the training activity is the responsibility of a specific group or is organization-wide.	There are times when a training need may be specific to a group or even just one team. In those cases, the group or team will have the responsibility to meet that need.
Determine the priority of the identified training needs.	Criteria for prioritizing could include • criticality of the skill or knowledge for delivering the service(s) • number of people who already have the skill or knowledge vs. those who need it (depth of skill or knowledge in the organization) • total number of people who need the skill or knowledge
Create a list of prioritized training needs.	

Table 3: Awareness Needs Analysis

Activity	Details
Review identified awareness needs.	Review the identified awareness needs to determine if the program can meet them.
Categorize the awareness needs.	Example categories include • resilience requirements • organizational policies • vulnerabilities under watch • laws and regulations • service continuity plans
Create a table showing awareness needs by category and personnel groups.	Gain a better understanding of the extent of the awareness need across personnel groups as well as categories of awareness needs of the different personnel groups.
Determine if the awareness activity is the responsibility of a specific group or is organization-wide.	There are times when an awareness need may be specific to a group of personnel or even just one team. In those cases, the group or team will have the responsibility to meet that need.
Determine the priority of the identified awareness needs.	Criteria for prioritizing could include • criticality of the awareness information for delivering the service(s) • risks associated with personnel not being aware of the needed information • total number of people who need to be exposed to the awareness information
Create a list of prioritized awareness needs.	

Output of Section IV

	Output	Guidance
✓	Identified training needs	• Table of training needs showing categories and number of personnel needing the training • List of training needs ordered by priority
✓	Identified awareness needs	• Table of awareness needs showing categories and personnel grouping • List of awareness needs ordered by priority
✓	Recommended training and awareness actions	• List of recommended training and awareness actions

V. Conduct Training and Awareness Activities

Before You Begin

The following checklist summarizes the tasks you will need to complete and the information you will need to gather before you can begin conducting training and awareness activities.

	Input	Guidance
✓	Training and awareness plan	• What were the goals and objectives of the plan, and what is the expected timeline?
✓	Identified training needs	• Table of training needs showing categories and number of personnel needing the training • List of training needs ordered by priority
✓	Identified awareness needs	• Table of awareness needs showing categories and personnel grouping • List of awareness needs ordered by priority
✓	Recommended training and awareness actions	• List of recommended training and awareness actions

Step 1. Establish and maintain support functions for training and awareness.

If the organization has an established training program, there may already be training and awareness support functions in place. If not, then the organization needs to establish certain support functions. First, a library structure needs to be created for storing training and awareness materials. The structure should allow for versioning of materials such as presentations and internally developed course materials (course modules, handouts, exercises, etc.).

Also, the organization should establish a tracking and record-keeping system. Training and awareness records could include

- course or training activity with date conducted
- course or training activity attendees
- course instructors
- awareness activities with date conducted, completed, or disseminated
- personnel attending awareness activity (if a presentation)
- employee training records

In addition, a tracking mechanism for tracking progress against the planned training and awareness activities needs to be in place.

Other support functions include

- logistical functions, such as email distribution lists, classroom scheduling, and instructor scheduling systems
- measurement and evaluation activities (see Section VI)

Step 2. Develop training and awareness materials.

The organization can use the lists of prioritized training and awareness needs to plan how those needs will be met. Training can be accomplished through several different approaches, such as

- classroom training
- guided self-study
- on-the-job training
- mentoring programs

In addition to determining the approach to use, the organization needs to decide whether it will acquire the training through a third-party provider or develop the training itself. Although many training needs can be met through third-party providers, certain organization-specific training (such as process-related training) should be developed internally.

Similarly, awareness activities can be accomplished through several different approaches, such as

- poster campaigns
- newsletters
- email messages
- presentations for organization-wide or team meetings
- trainer-facilitated sessions

Again, the organization needs to decide whether it will acquire third-party services to support the awareness activities or do the work in-house. If the organization decides to develop training and awareness materials in-house, it is recommended that the organization follow a development approach. Table 4 shows an example development approach.

Table 4: Example Training and Awareness Materials Development Approach

Development Item	Purpose
Product Plan	Documents the need for the training or awareness material, intended audience, materials needed, resources needed, and development and delivery constraints
Product Design	Documents a high-level design and a list of the elements that need to be developed (e.g., for a course, presentation materials, exercises, handouts)
Training or Awareness Materials	Specifies materials developed to conduct the training or awareness activity
Verification & Validation of Materials	Defines tests, pilots, prototypes, or other activities to make sure the materials are ready for full-scale production and deployment
Disposal/Sustainment	Explains the removal of items once they have been updated or are no longer useful to your organization

Initial planning for the development of training and awareness materials can reduce the amount of rework caused by uncertain requirements early in the development cycle.

Step 3. Procure third-party provider services.

When an organization decides to use third-party providers to develop or deliver training or awareness activities, it should ensure that the training or awareness activities delivered address the needs of the organization and are of the quality expected. Also, the organization needs to establish an agreement with that supplier. This may be as simple as a license fee or a registration fee for attending a course, or it may be more complex and require a more formal contract agreement.

Step 4. Conduct training and awareness activities.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/ Subcategory
Goal 2 – Awareness and training activities are conducted.	
1. Are cyber security awareness activities for the critical service conducted? [OTA:SG2:SP1]	**PR.AT-1: All users are informed and trained**
2. Are cyber security training activities for the critical service conducted? [OTA:SG4.SP1]	**PR.AT-1: All users are informed and trained**

Training and awareness activities need to be scheduled. For a class, it is best if the schedule provides at least a three-month lead time before an actual activity is conducted. This allows time to prepare materials, prepare instructors, arrange logistics, and settle attendee availability. Other activities also need to be scheduled to ensure that the activity developer is available and that materials production is completed. When scheduling activities, consider other scheduled organizational activities, holidays, and potential vacations or other staff absences. Training activities and awareness activities can be conducted through significantly different approaches (from classroom training to email messages), which can allow for some flexibility in scheduling to meet situational needs.

The conduct of training and awareness activities should be tracked against the plan and scheduled to ensure the training and awareness objectives are met. Evaluation of training and awareness activities provides feedback on their effectiveness. See Section VI, Improve Training and Awareness Capability, for a discussion on evaluation techniques and analysis.

Outputs of Section V

	Output	Guidance
✓	Tracking records and material	• Materials used, personnel trained, and initial feedback
✓	Product development artifacts	• Materials used to develop the training and awareness products
✓	Training and awareness activity materials	• Materials that are used to conduct the training and awareness activities
✓	Training and awareness activities schedule	• Schedule of when training and awareness activities are conducted

VI. Improve Training and Awareness Capability

Before You Begin

The following checklist summarizes the tasks you will need to complete and the information you will need to gather before you can begin assessing training and awareness.

	Input	Guidance
✓	Training and awareness plan	What were the goals and objectives of the plan?
✓	Tracking records and material	What materials were used, who was trained, and what was the initial feedback?
✓	Interviews with employees and supervisors	What observations can the employee provide about the effectiveness of the training and awareness activity after the employee has performed the job?

Step 1. Establish a plan to evaluate the training and awareness program.

Evaluation of the training and awareness program should be planned for while the training and awareness program is being developed and its materials are being planned and designed.

Key personnel performing the evaluation should have the following responsibilities:

- developing the evaluation process and scope
- analyzing and assessing the training and awareness activities
- managing internal/external entities during the evaluation process
- summarizing the evaluation results

Stakeholders include

- owners of enterprise-level cybersecurity policies and procedures
- service or asset owners
- supervisors of employees with cybersecurity responsibilities
- external entities such as trainers and those developing training and awareness materials
- staff performing the work

Depending on the scope of the assessment, personnel performing the evaluation or stakeholders supporting it may require specialized training.

Artifacts and materials produced in the planning of training and awareness activities will support the evaluation of the overall program's effectiveness. The organization can also require data to be collected before and during these activities.

When evaluating the effectiveness of training and awareness activities, plan to collect measures that allow the examination of four specific aspects:

- the appropriateness of the learning conditions (in the employee's opinion)
- what, specifically, an employee was expected to learn from each training or awareness activity
- how the performance or behavior of the employee changed following specific training and awareness activities
- the effectiveness of a specific training and awareness activity compared to other options

Collection of this data will require access to those who plan and administer the training and awareness activities, the employees who will participate in those activities, and the supervisors who will select and evaluate the employees who will participate.

The data collected should enable the organization to analyze the program against four desired outcomes:

- Employees are better able to perform their jobs.
- Supervisors are better able to assess changes to their employees' on-the-job performance.
- The organization feels confident that the employees are performing activities in a way that demonstrates a resilient organization (e.g., meet the goals and objectives).
- The training and awareness activities can be improved.

Step 2. Evaluate training and awareness program and analyze results.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/ Subcategory
Goal 2 – Awareness and training activities are conducted.	
3. Is the effectiveness of the awareness and training programs evaluated? [OTA:SG2.SP3, OTA:SG4.SP3]	**PR.AT:** The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.
	PR.IP-7: Protection processes are continuously improved

Once the organization has developed a plan to collect the data needed to evaluate the training and awareness program, it should implement the plan. Data may be collected continuously or after discrete events, such as at the end of a class or presentation. But those evaluating the training and awareness plan should establish a schedule that supports the collection, consolidation, and analysis of data and enables Step 3 (Improve the Process).

Collect data.

Using the objectives that define training and awareness activities, those evaluating these activities organize the data to support a regular evaluation cycle. Recall that the previous step outlined the measures that support the analysis of the program. Data collected to support this analysis comes from four sources:

- the employees being trained
- the supervisors who identified the training shortfalls and can observe changes in employee behavior
- corporate leadership that establishes performance objectives to accomplish the organization's mission
- those who actually conduct the training and awareness activities

Table 5 lists the types of data that might be collected, describes the data, and suggests what the data might be used to determine.

Table 5: Evaluation Measures

Type of Data	Data Description	Data Determines…
Employee Satisfaction Survey (administered immediately after activity, responses on a scale of poor to excellent)	• Adequacy of learning environment • Adequacy of instructor/learning activity • Extent to which the employee was prepared	• Fulfillment of the conditions • Relevancy of training to employee • Adequacy of articulation of prerequisites for this training
Learning and Teaching Effectiveness (performance test just prior to successful completion of the course)	• Results of performance testing based on activity just completed	• Fulfillment of the training objectives • Appropriateness of the activity to the performance desired • Comparison to similar activities
Employee Performance Effectiveness (60-90 days after training and awareness activity)	• Structured questionnaire to evaluate before-and-after performance of tasks relevant to activity being evaluated • Measure of quantitative improvement • Measure of qualitative improvement	• Effectiveness of training and awareness activity • Efficiency gains toward meeting corporate objectives • Comparison to similar activities
Training and awareness program effectiveness	• Value of improvement due to training and awareness activities • Cost of training and awareness activities	• Improvements achieved by the organization • Allocation of resources for training and awareness activities

The organization must recognize that the evaluation process is an information-gathering process. The evaluations allow the organization to measure the effectiveness of training and awareness activities and will ultimately work to achieve organizational performance and efficiency objectives.

Identify weaknesses.

Evaluators should be looking for and documenting the weaknesses such as the following (for illustration only; these may not represent weaknesses in all organizations):

- conditions—Example: training was conducted using equipment that was no longer in the organization's active inventory.
- ineffective training activity—Example: employees are consistently unable to demonstrate skills by the end of the block of instruction.
- insufficient impact on employee behavior—Example: despite mandatory phishing awareness training, a significant percentage of employees falls victim to a simulated phishing email.

Leverage existing assessment results.

Evaluations should leverage existing documentation from other domains, such as the results of service continuity exercises, incident handling responses, and risk assessments. Looking back on existing documentation from these areas could give the organization useful insight on how training and awareness objectives have or have not been satisfied.

See the Service Continuity Resource Guide, Volume 6 of this series. Also see the Service Continuity (SC) process area in the CERT-RMM for additional information on conducting service continuity exercises.

See the Incident Management Resource Guide, Volume 5 of this series. Also see the Incident Management and Control process area in the CERT-RMM for additional information on handling incidents.

See the Risk Management Resource Guide, Volume 7 of this series. Also see the Risk Management process area in the CERT-RMM for additional information on managing risks.

Step 3. Improve the process.

Training and awareness capabilities must be kept current and up to date; the manner in which the training and awareness material is delivered must be effective in the eyes of those who are being trained.

The results of a completed evaluation will enable the organization to make informed decisions about improving the training and awareness plans and strategies. Once the organization has identified the problem areas, it can begin to identify updates to existing training and awareness activities and propose new activities.

Use the feedback loop.

As depicted in Figure 1 (page 4), an organization's evaluation of its training and awareness activities is an ongoing process. As technology and processes change, so must the training and awareness program. The organization must always assess these changes so it can properly manage decisions related to operational resilience.

The organization should leverage other domains during the feedback loop. Lessons learned from the deployment of other processes may yield training and awareness needs that will enable the organization to increase its operational resilience. Domains to consider include the following:

- incident management—As incidents are investigated, gaps in the training and awareness program will become known. These gaps should be discussed during the post-incident brief, and recommendations to improve the training and awareness program should be made.
- risk management—The organization's normal risk review sessions will reveal new risks. The revealed risks that can be mitigated by training should be fed into the training and awareness plan.
- service continuity—As disaster recovery and business continuity plans are developed and exercised, failures should be documented, and recommendations for new training and awareness objectives and activities should be fed into the training and awareness program.

The list above provides examples for the organization to consider. Domains not listed, however, can provide inputs to the training and awareness plan.

KEY TAKEAWAY: *The organization should always look to improve its operational cyber resilience by leveraging other domains and their outputs.*

Step 4. Update training and awareness materials.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/ Subcategory
Goal 2 – Awareness and training activities are conducted.	
4. Are awareness and training activities revised as needed? [OTA:SG1.SP3, OTA:SG3.SP3]	**PR.AT:** The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.
	PR.IP-7: Protection processes are continuously improved

The final step in the evaluation process enables the organization to implement the updates and new training and awareness activities. The process outlined above provides the due diligence an organization needs in order to confidently assess the training and awareness program and make changes based on the evaluation.

As updates are made, it is important for the organization to schedule follow-on reevaluations to ensure that the updates and new activities are effectively achieving training and awareness objectives.

Output of Section VI

	Output	Guidance
✓	Evaluation report	• Outlines the areas below
✓	Evaluation of changes to on-the-job performance	• Contains changes reported by both employees and their supervisors
✓	Data	• Improves both learning and teaching
✓	Return on investment	• Supports resource allocation to the most effective training and awareness activities
✓	Review of material	• Maintains currency
✓	Remediation plans	• Ensures training and awareness objectives are satisfactorily addressed

VII. Conclusion

Establishing and supporting an ongoing training and awareness program enables your organization to meet its goals and objectives. The training and awareness program helps to ensure that your organization can sustain its critical services and meet its responsibility to its stakeholders and its contribution to national critical infrastructure.

The variety of documentation, standards, and guidelines developed to address training and awareness is extensive, but there are just a few straightforward foundational activities that these items share, such as establishing a training and awareness program, planning, identifying training and awareness needs, conducting training and awareness activities, and improving the program. This document is organized around those common foundational activities. The approach taken is to provide an outline of *what* should be done to establish and maintain a training and awareness program, rather than *how* to do it.

The following documents provide broad program guidance:

- *NIST Special Publication 800-16 Revision 1 (2nd Draft Version 2), A Role-Based Model For Federal Information Technology/Cyber Security Training* provides information on a training methodology for the development of training for personnel with cybersecurity responsibilities.
- The *CERT-RMM* [Caralli 2010] is the basis for the CRR and contains more in-depth guidance for establishing practices. The Operational Training and Awareness process area provides a detailed description of practices and goals associated with training and awareness.

For more information about the Cyber Resilience Review, please email the Cyber Security Evaluation Program at CSE@hq.dhs.gov, or visit the website of the Office of Cybersecurity and Communications at http://www.dhs.gov/office-cybersecurity-and-communications.

Appendix A. Training and Awareness Resources

National Institute of Standards and Technology (NIST)
http://www.nist.gov/index.html

- NIST Computer Security Division, Computer Security Resource Center
  http://csrc.nist.gov/
    - NIST Special Publication 800-16 Revision 1 (2nd Draft Version 2), A Role-Based Model For Federal Information Technology/Cyber Security Training

Software Engineering Institute, CERT Division
http://www.sei.cmu.edu/

CERT-RMM
http://www.cert.org/resilience/products-services/cert-rmm/index.cfm

Appendix B. CRR/CERT-RMM Practice/NIST CSF Subcategory Reference

Table 6 cross-references CRR Training and Awareness Domain goals and practice questions to the NIST CSF Categories/Subcategories and the sections of this guide that address those questions. Users of this guide may wish to review the CRR Question Set with Guidance available at https://www.us-cert.gov/ccubedvp for more information on interpreting practice questions. The NIST CSF available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf provides informative references for interpreting Category and Subcategory statements.

Table 6: Cross-Reference of CRR Goals/Practices and NIST CSF Categories/Subcategories Reference and the Training and Awareness Resource Guide

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/ Subcategory	Training and Awareness Resource Guide Reference
Goal 1 – Cyber security awareness and training programs are established.		—
1. Have cyber security awareness needs been identified for the critical service? [OTA:SG1.SP1]	**PR.AT-1:** All users are informed and trained	Section IV, Step 4
2. Have required skills been identified for specific roles (administrators, technicians, etc.) for the critical service? [HRM:SG1.SP2]	**PR.AT-1:** All users are informed and trained	Section IV, Step 2
3. Are skills gaps present in personnel responsible for cyber security identified? [OTA: SG3.SP1]	**PR.AT-1:** All users are informed and trained	Section IV, Step 2
4. Have training needs been identified? [OTA: SG3.SP1]	**PR.AT-1:** All users are informed and trained	Section IV, Step 4
Goal 2 – Awareness and training activities are conducted.		—
1. Are cyber security awareness activities for the critical service conducted? [OTA:SG2:SP1]	**PR.AT-1:** All users are informed and trained	Section V, Step 4
2. Are cyber security training activities for the critical service conducted? [OTA:SG4.SP1]	**PR.AT-1:** All users are informed and trained	Section V, Step 4
3. Is the effectiveness of the awareness and training programs evaluated? [OTA:SG2.SP3, OTA:SG4.SP3]	**PR.AT:** The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements. **PR.IP-7:** Protection processes are continuously improved	Section VI, Step 2
4. Are awareness and training activities revised as needed? [OTA:SG1.SP3, OTA:SG3.SP3]	**PR.AT:** The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements. **PR.IP-7:** Protection processes are continuously improved	Section VI, Step 4

Endnotes

1. For more information on the *Cyber Resilience Review*, please contact the Cyber Security Evaluation Program at CSE@hq.dhs.gov.
2. *CERT-RMM*. "Glossary of Terms" [Caralli 2010].
3. Caralli, R. A.; Allen, J. A.; & White, D. W. *CERT®-RMM: A Maturity Model for Managing Operational Resilience (CERT-RMM, Version 1.1).* Addison-Wesley Professional, 2010. For more information on the CERT-RMM, please visit http://www.cert.org/resilience/rmm.html.
4. "Operational Training and Awareness Process Area." *CERT-RMM* [Caralli 2010].
5. The *CERT-RMM* (EF:SG1) [Caralli 2010] discusses the need for resilience activities to meet strategic objectives.
6. Gates, L. P., *Strategic Planning with Critical Success Factors and Future Scenarios: An Integrated Strategic Planning Framework* [CERT 2010] discusses strategic planning.
7. Gates, L. P., *Strategic Planning with Critical Success Factors and Future Scenarios: An Integrated Strategic Planning Framework* [CERT 2010] discusses strategic planning.
8. The *CERT-RMM* (OTA:SG1and SG3) [Caralli 2010] discusses how to identify management directives and organizational guidelines.
9. The *CERT-RMM* (OTA:SG1and SG3) [Caralli 2010] discusses how to identify management directives and organizational guidelines.
10. The *CERT-RMM* (OTA:SG1:SP1and SG3:SP1) [Caralli 2010] discusses prioritizing objectives.