CRR Supplemental Resource Guide

Volume 10

Situational 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-0003285

Table of Contents

I. Introduction

Series Welcome

Welcome to the CRR Resource Guide series. This document is one of 10 resource guides developed by the Department of Homeland Security's (DHS) Cyber Security Evaluation Program (CSEP) 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*, specific to IT operations. Operational resilience is 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 and during times of operational stress and crisis. The guides were developed for organizations that have participated in a CRR, but any organization interested in implementing or maturing operational resilience capabilities for critical IT services will find these guides useful.

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
10. **Situational Awareness** ⇦***This guide***

The objective of the CRR is to allow organizations to measure the performance of fundamental cybersecurity 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 each 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 leverage complementary materials and suggestions to optimize their adoption approach. For example, the resource guides for incident management, vulnerability management, service continuity, risk management, and external dependencies management can provide insight into other areas that exchange information with, and have process linkages to, situational awareness.

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. See Appendix B for a cross reference between the CRR and this guide.

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

- create a situational awareness plan
- perform data collection and analysis for situational awareness
- communicate situational awareness information
- improve situational awareness processes and technology

More specifically this guide

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

The guide is structured as follows:

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

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

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

III. Plan for Situational Awareness—Highlights the elements necessary for an effective situational awareness plan.

IV. Collect and Analyze Situational Awareness Data—Presents an approach for identifying and managing the requirements for situational awareness data collection and analysis, including recommended categories of information to be monitored to assure organizational resilience and an approach for analyzing situational awareness information.

V. Communicate Information Needed to Make Appropriate Decisions—Outlines a process that defines steps necessary to manage the communication of information to appropriate staff, enabling them to make informed decisions and identify follow-up actions.

VI. Improve Situational Awareness Processes and Technology—Provides an approach for reviewing and improving the organization's situational awareness capability.

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

Appendices

A. Situational 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 situational awareness. Executives who establish policies and priorities for situational awareness, managers and planners who are responsible for converting executive decisions into plans, and staff responsible for implementing the plans and conducting situational 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 the endnotes.

II. Situational Awareness

Overview

> *The purpose of situational awareness is "to actively discover and analyze information related to immediate operational stability and security and to coordinate such information across the enterprise to ensure that all organizational units are performing under a common operating picture." CRR*[4]

Situational awareness provides an organization an understanding of its critical service's operating environment and the environment's impact on the operation of the critical service. This understanding provides stakeholders with a sufficiently accurate and up-to-date understanding of the past, current, and projected future state of a critical service and supports effective decision making in the context of a common operating environment. This includes understanding the assets and other services that affect or depend on the critical service. The representation or picture of the state of a critical service (including the condition of its supporting assets, the performance of its high-value physical and cyber processes, and events detected and responded to by its physical and cybersecurity safeguards) is presented to stakeholders in the context of the threat environment (internal and external) and the resulting risks to the critical service's mission.

> *Situational awareness is commonly defined as "the perception of elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future." Endsley (1995)*[5]

The situational awareness process establishes a *common operating picture* (COP) by collecting, fusing, and analyzing data to support automated or human decisions about appropriate actions to prevent disruption of a critical service or to restore the service to proper function. This COP is shared through timely communication and presentation of the results of the data analysis to appropriate decision makers (people or machines) in a form that aids human comprehension (e.g., using data visualization techniques, appropriate use of alarms) and allows operators or other personnel to quickly grasp the key elements needed for good decision making.

> *When building a resilience program in your organization, other processes need to be considered. Much of the situational awareness process involves fusing and improving the information for use in decision making, not telling stakeholders what to do. An important part of situational awareness is to establish the context for the information.*

The COP should be accurate and actionable (appropriate for supporting good decisions and actions). However, different members of an organization likely need different, and not necessarily complete, views of the operational environment. Depending on how it is presented, a complete picture could present too much information and overload a human decision maker. Operators should not be presented with a massive data dump; rather, operators should see only what's important, which is determined by the risk strategy and overall risk picture.

Communication between situational awareness and other organizational processes is bi-directional. Other processes report information, such as vulnerabilities, incidents, and risk management decisions, to the situational awareness process. At the same time, the situational awareness process contributes the information, or improves its quantity or quality, needed by other processes that inform decision making or appropriate actions.

Communication among processes relies on their linkages. These linkages can be simple, such as reporting of suspicious events to the incident response team. They can also be complex, such as asset and controls management processes that include an intrusion detection system (IDS) that monitors assets and services deemed important by the risk management process and alerts those who can take mitigating steps.

Linkages to Other CRR Domains

Broadly speaking, the various processes within an organization intake data, convert it into usable information, and share it with other processes. This flow of data and information helps define the processes' relationships many of which involve situational awareness.

Asset management processes lay the foundation for situational awareness by identifying the critical services and associated assets (with linkage also to risk management) that the situational awareness process should concentrate on.

Risk management is the foundation for eliciting situational awareness requirements and the lens through which situational awareness information is interpreted and communicated. Risk management also involves a few processes. Vendors, the vulnerability management team, or other sources may communicate the existence of a vulnerability to the organization. The situational awareness process provides this information to asset management, which determines which assets are affected by the vulnerability and the potential risks to the critical service. This information feeds the situational awareness process, which feeds it to the risk management team. With this situational awareness information in hand, the risk management team can prioritize the risks posed by the vulnerability relative to other risks and, if necessary, increase the urgency of remedial action, such as requesting a patch or workaround from a vendor.

The situational awareness process feeds data to the incident management process, which may correlate it with information from other CSIRTs and, when appropriate, declares an incident and communicates it to relevant stakeholders.

The external dependencies management process receives situational awareness information on potentially risk-increasing events or changes involving external business and technical relationships (e.g., vendors/suppliers and service providers), partners, and collaborators (e.g., ISACs). Some external entities provide situational awareness directly to the organization. To ensure that the organization receives the situational awareness data it needs, the organization must collaborate with those critical external entities.

The four-phase situational awareness process (Figure 1) comprises the activities by which an organization plans for, conducts, communicates, and improves situational awareness to ensure that the organization's operational cyber resilience requirements and goals are met.

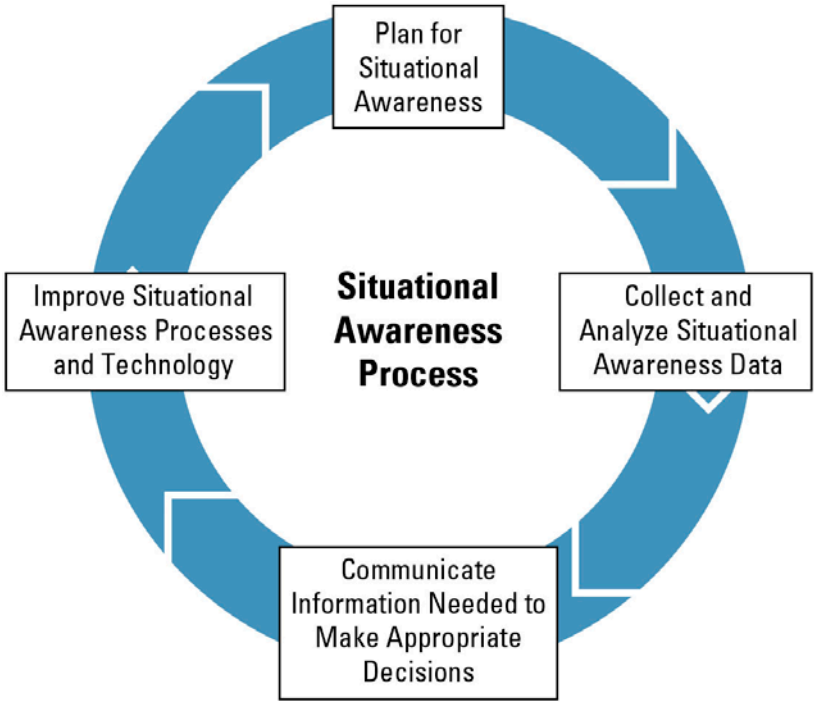

Figure 1: The Situational Awareness Process

We have broadly described situational awareness in terms of the domain's purpose as described by the CRR: to discover and analyze information related to immediate operational stability and security and to communicate such information across the enterprise. However, the situational awareness questions in the CRR assessment all focus on the monitoring and communication of what is arguably a subset of situational awareness information: threat information. As a result, this CRR resource guide focuses on the following situational awareness activities:

- collecting and analyzing data from external threats
- identifying suspicious behavior of potential internal threats
- communicating threat information
- participating in threat-sharing communities

The high-level outline below highlights the four phases of this process and points the reader to the corresponding details in this guide.

Situational Awareness Process

Plan for Situational Awareness

Situational awareness is a support process that ensures staff members and external stakeholders have the information they need to perform their work in other processes such as incident management, controls management, vulnerability management, service continuity management, and risk management. Situational awareness takes place at various levels of an organization. Enterprise-level situational awareness addresses organization-wide needs. Specific situational awareness activities are developed and implemented at the organizational level (e.g., business unit or team) where they are needed. For situational awareness at any level of the organization, management support is essential. With management support, processes are defined to

identify and implement situational awareness activities that make available the information on potential threats to the continued resilience of services.

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

Important activities while planning for situational awareness include the following:

- Obtain support for situational awareness planning.
- Establish a situational awareness program strategy.
- Establish an approach to collecting and analyzing situational awareness data.
- Establish an approach for communicating situational awareness information.
- Establish a situational awareness plan.

Collect and Analyze Situational Awareness Data

The identification of situational awareness requirements provides critical information for the development of a situational awareness program. If the organization has an established situational awareness program, there may already be a requirements analysis process in place. Still, the organization should review the previously identified requirements to ensure they include those specific to cyber resilience and, periodically, to see if any of the requirements have changed. Establishing situational awareness requirements must involve the stakeholders for whom situational awareness information must be collected and to whom it must be communicated.

Situational awareness requirements specific to cyber resilience can be derived from other domain plans (e.g., vulnerability management, incident management, and service continuity management). Those plans include a list of critical information needed to perform the planned work. The organization should also review domain plans to identify the activities needed to support cyber resilience, which inform the organization's situational awareness requirements. Once situational awareness requirements are identified, an organization must analyze those requirements to determine what actions it will take to resolve gaps.

Important activities for collecting and analyzing situational awareness data include the following:

- Establish situational awareness data collection and analysis requirements.
- Establish an approach to collecting and analyzing situational awareness data.
- Establish and maintain an infrastructure to support situational awareness monitoring activities.
- Collect, record, and analyze information.

Communicate Information Needed to Make Appropriate Decisions

To be effective, information collected through the situational awareness activities must be effectively communicated to the stakeholders who need that information to make informed decisions regarding the cyber resilience of services.

Important activities for communicating situational awareness information include the following:

- Establish situational awareness communication requirements.
- Establish communication standards and guidelines.
- Establish and maintain an infrastructure to support situational awareness communication activities.
- Communicate situational awareness information.

Improve Situational Awareness Processes and Technology

Successfully managing risks to the critical service depends largely on the effectiveness of the organization's situational awareness processes and technology. In an environment of increasing cyber and physical threats, it is particularly important for the organization to continually improve its situational awareness capability.

Important activities in the improvement of situational awareness processes and technology include the following:

- Review overall situational awareness program effectiveness.
- Identify updates and improvements to the situational awareness program.
- Make improvements to the processes and technology

Summary of Steps

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

Plan for Situational Awareness

1. Obtain support for situational awareness.
2. Establish a situational awareness program strategy.
3. Establish an approach to collecting and analyzing situational awareness data.
4. Establish an approach for communicating situational awareness information.
5. Establish a situational awareness plan.

Collect and Analyze Situational Awareness Data

1. Establish situational awareness data collection and analysis requirements.
2. Establish an approach to collecting and analyzing situational awareness data.
3. Establish and maintain an infrastructure to support situational awareness monitoring activities.
4. Collect, record, and analyze information.

Communicate Information Needed to Make Appropriate Decisions

1. Establish situational awareness communication requirements.
2. Establish collection standards and guidelines.
3. Establish and maintain an infrastructure to support situational awareness communication activities.
4. Communicate situational awareness information.

Improve Situational Awareness Processes and Technology

1. Review overall situational awareness program effectiveness.
2. Identify updates and improvements to the situational awareness program.
3. Make improvements to the processes and technology.

Organizations that already have situational awareness plans can assess and improve them by using the guidance in this resource guide.

III. Plan for Situational 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 to develop a situational awareness program.

	Input	Guidance
✓	Scoping statement	This statement defines what the situational awareness program and plans need to address. The plans could be scoped to cover, at a minimum, all mission-essential organizational services. Organizations that are not sure where to start should focus on the most essential services and the areas that directly affect their performance. This approach may allow an organization to address the areas of greatest risk first and mitigate their impact while situational awareness practices are being more fully developed. If your organization has participated in a CRR, it may be beneficial to begin with the essential service addressed during the CRR. See Appendix B for a cross reference between the CRR and this guide.
✓	Lists of stakeholders	The list of stakeholders should be aligned to the scoping statement and include all appropriate internal and external entities. Potential candidates include • service/business owners within the organization • business partners and vendors • technology and infrastructure owners in the organization • law enforcement and other first responder organizations • technology vendors • regulators and auditors • customers and providers who may be impacted in the event of service interruption
✓	Management support	• An endorsement by senior management for establishing a situational awareness program and implementing processes
✓	An understanding and acknowledgement of an acceptable approach to situational awareness	• Acknowledgement of the intended approach to situational awareness, including stakeholder expectations about acceptable strategies and objectives
✓	Externally imposed requirements for situational awareness	• Regulatory requirements defining mandatory situational awareness requirements and other needs • Service-level agreement requirements with other organizations with whom situational awareness is required
✓	Assignment of responsibility for situational awareness	• Job descriptions and performance reviews for roles that have responsibilities for situational awareness, for example, executive ownership, decisions, and communication
✓	Budget for situational awareness	• Identification of available funds and resources to perform situational awareness: o staffing resources o tools (applications and associated hardware) o third-party support o technology to support resilience requirements
✓	Linkage to other plans	• Coordination of situational awareness planning, monitoring, and communication with other processes

Step 1. Obtain support for situational awareness.

Obtaining support from management, in the form of resources (budget and staffing) and organizational commitment, is essential to ensuring the situational awareness plan is effectively implemented. A top-down approach can also help ensure the situational awareness program meets the resilience objectives of the organization.

The level of management support required depends on the scope of the situational awareness program being implemented. Senior-executive-level support is necessary for a situational awareness plan that addresses the entire organization. Smaller implementations, such as those at the business unit or team levels, may require sponsorship only from the management responsible for that particular organizational level. To illustrate this, consider an electric utility company that has four main services: generation, transmission, distribution, and business support. Each service could implement its own situational awareness program. 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, situational awareness planning is usually iterative. As the other phases of the situational awareness process are completed (data collection and analysis, communicating situational awareness information, and improvement), the plan will need to be reviewed and revised. Eventually, situational awareness re-planning may be done periodically.

Step 2. Establish a situational awareness program strategy.

Establishing a high-level strategy that focuses on long-term goals can be the foundational activity for any program. Establishing a strategy for situational awareness helps the organization develop a situational awareness program that reflects the priorities of the enterprise, operating units, and specific critical services. The following steps illustrate an approach for establishing the strategy for a situational 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.[6] 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.[7] Large enterprises may have strategic plans at multiple levels within the organization, such as the enterprise and operating-unit levels. In this document, a plan refers to a set of activities, with associated assignments and resources, that is designed to accomplish an objective. It is more detailed and has a shorter timeframe than a strategy.
   - critical success factors (CSFs)—A small number of areas in which an organization must consistently perform well to meet its goals and mission.[8] CSFs illustrate what the organization considers its top priorities in achieving its goals.
   - legal and regulatory obligations—Frequently sources of insight into requirements placed on the organization by external entities.[9]
   - internal policies and standards—Policies and procedures developed by the organization to promote acceptable behaviors and practices.[10]

B. Identify complementary strategies and plans that support and rely on situational awareness activities. Such strategies and plans include, for example,

- risk management
- asset management
- incident management
- vulnerability management
- service continuity management

C. Define and document situational awareness program objectives. Situational awareness program objectives are derived from the management directives and organizational priorities identified above.

D. Prioritize situational awareness program objectives. Situational awareness program objectives should be prioritized based on their potential to affect operational resilience.[11] These priorities will help the organization allocate resources.

The resources available to an organization for situational awareness will influence the selection of the situational awareness program strategy, which should

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

The purpose of a situational awareness program is to identify specific activities that can implement and support the situational awareness objectives. The following steps illustrate an approach for integrating situational awareness objectives specific to cyber resilience in an existing situational awareness program:

i. To avoid redundancy, review the existing situational awareness program activities before implementing new ones.
ii. Assess the effectiveness of existing situational awareness program activities, using sufficient evidence. This review is often completed as a by-product of auditing or feedback and measurement activities.
iii. Establish new situational awareness program activities to fill the gaps left by existing activities.
iv. Confirm that the proposed revised situational awareness program effectively meets all of its objectives, and assign responsibility, typically to operating-unit managers, for implementing new activities.

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

Step 3. Establish an approach to collecting and analyzing situational awareness data.

The organization must establish how it will collect and analyze situational awareness data to determine how it will meet organizational goals. Table 1 outlines an approach to collecting situational awareness data, and Table 2 outlines an approach to analyzing the collected data. Procedures should be implemented to ensure the timeliness, consistency, and accuracy of threat information.

Table 1: Collecting Situational Awareness Data

Activity	Details
Review what data is currently being collected.	Data may be collected by different processes, for example, • vulnerability management • risk management • enterprise-level processes
Identify information needs.	Identify and prioritize types of data that are needed.
Identify sources of data.	Data sources can be internal or external and should be from trusted sources. Sources may include • audit logs • incidents, faults, and alarms • maintenance requirements for hardware • service-desk reports
Determine data storage requirements.	Data storage requirements include • categorization of data by type, timeliness and granularity • data security needs and access restrictions • disposition of data when no longer required

Table 2: Analyzing Situational Awareness Data

Activity	Details
Understand situational awareness data analysis that is currently being done.	Review the techniques and tools currently being used. Review the output to understand the reports/results being communicated.
Identify situational awareness data analysis needs.	Identify situational awareness data analysis needs for cybersecurity, for example, • trend analysis • correlation • exception reports • simulation and modeling • impact analysis
Identify tools needed for data analysis.	Tools needed for data analysis can include • statistical analysis tools • simulation and modeling tools • data visualization tools
Determine categories of alerts.	The analysis of the situational awareness data provides information on the current COP. Threat information needs to be categorized based on impact, probability, and timeframe.

Step 4. Establish an approach for communicating situational awareness information.

The organization must communicate situational awareness information about events or threats that can adversely impact the organization's critical services. Frequently, this is accomplished by building a *common operational picture* (COP). The COP provides a means of communicating threat information to stakeholders in an appropriate and timely manner and serves as the basis for making good decisions and taking proper actions. Table 3 outlines an approach to communicating situational awareness information.

Table 3: Communicating Situational Awareness Information

Activity	Details
Identify different types of communications based on criticality and stakeholders affected.	Different types of threat information often need to be communicated differently. Imminent, high-impact situations often need to be communicated quickly and widely. Other types of threat information only need to be communicated to a few key people.
Identify communication methods and channels.	Example methods include • threat communication standards and guidelines • standardized report templates • communication escalation protocols • communication channels (email, text, mobile phone, etc.)
Create a table showing stakeholders by category and types of communication they require.	Gain a better understanding of the extent of the communications needed by stakeholders across categories and the actual types of communications those stakeholders need.
Determine if the communication activity is the responsibility of the situational awareness process or is an organization-wide responsibility.	There are times when a situational awareness communication is beyond the scope of the situational awareness process. In those cases, an organization-wide group will be responsible for communicating the information.

Step 5. Establish a situational awareness plan.

A situational awareness plan describes how the organization will collect, analyze, and communicate situational awareness information. The objectives of the plan are translated into specific activities assigned to individuals or groups. A situational awareness plan should address

- the organization's approach to situational awareness
- the structure of the situational awareness process
- the requirements and objectives of the situational awareness process
- a description of how the organization will collect, analyze, and communicate situational awareness information
- the roles and responsibilities necessary to carry out the plan
- applicable training needs and requirements
- resources that will be required to meet plan objectives
- relevant costs and budgets associated with situational awareness activities

As the situational awareness plan documentation matures, the organization needs to address a few questions, presented in Table 4, about building an internal organizational infrastructure to support the plan's implementation.

Table 4: Situational Awareness Planning Questions

Questions
Do we know which roles/positions need to be filled now?
Do we know which 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 establish?
Do we have training events/resources in our budget and on our calendar?
When your answer to all of these is YES!—then you can feel comfortable that you have a plan.

Once your organization has documented its situational 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
✓	Enterprise guidance for situational awareness	• Organization-wide program, strategy, standards, and documentation for performing situational awareness activities
✓	Executive endorsement and oversight of situational awareness planning	• Situational awareness policy, standards, and program oversight or steering group
✓	Identified stakeholders for situational awareness	• All participants in the situational awareness process, including owners of services, will be aware of their roles and responsibilities
✓	Key foundational processes established	• Business impact and risk assessment processes defined to provide resilience requirements to the planning process
✓	Linkage to the other processes established	• Specifications of the interconnections and interactions among situational awareness and complementary processes so that they all work closely together to help ensure resilience
✓	Identified laws, regulations, and rules	• List of external requirements affecting the organization's situational awareness
✓	Processes for situational awareness	• Processes for situational awareness development, data collection, analysis, and communication, defined during the planning phase

IV. Collect and Analyze Situational Awareness Data

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 collecting and analyzing situational awareness data.

	Input	Guidance
✓	Scoping statement	• Definition of what the situational awareness program needs to address
✓	Lists of stakeholders	• The list of stakeholders identified during the planning phase
✓	Key foundational processes	• Definitions of the risk management and asset management processes include the development of resilience requirements for the critical service and its supporting assets. These foundational processes and the resilience requirements they produce are the basis for specifying requirements that guide the collection and analysis of situational awareness data.
✓	Linkage to the other processes established	• Specifications of the interconnections and interactions among situational awareness and complementary processes so that they all work closely together to help ensure resilience
✓	Identified laws, regulations, and rules	• List of externally mandated requirements affecting the organization's situational awareness data collection and analysis activities
✓	Processes for situational awareness	• Processes for situational awareness development, data collection, analysis, and communication, defined during the planning phase

Effective situational awareness depends on the timely collection of sufficiently accurate and inclusive risk-relevant data about the critical service (such as the condition of its supporting assets, the discovery of vulnerabilities to which it would be susceptible, the performance of its high-value physical and cyber processes, and the events detected by its physical and cybersecurity safeguards), the fusing of data from multiple internal and external sources, and the analysis of data, which often includes modeling and simulation. Done well, situational awareness improves stakeholders' understanding of the past, current, and projected future state of a critical service. The collection and analysis of situational awareness data, when effectively communicated to relevant stakeholders, supports automated or human decision-making concerning the appropriate actions for preventing the disruption of a critical service or restoring the service to proper function.

It is important that the organization's personnel to be trained to report suspicious or anomalous events to the incident response team. The organization must also have a well-publicized channel (phone number, web address) for such reports.

How and when tools such as instrumented logging will be activated depends on the organization's analysis of risk tradeoffs between storage and performance versus security. Regardless of this analysis, the organization will need to assign resources (human and machine) to regularly analyze logs. Collecting sufficient situational awareness data and devoting ample resources to its analysis provides the information necessary for mitigating the potential impacts of adverse events and improving security based on the lessons learned.

The following steps describe the activities for effectively collecting and analyzing situational awareness data in order to construct a COP that supports appropriate decision-making regarding the prevention or mitigation of risks to the critical service.

Step 1. Establish situational awareness data collection and analysis requirements.

Collecting and analyzing situational awareness data and building a COP provides a body of threat information that, when communicated to stakeholders in an appropriate and timely manner, serves as the basis for making good decisions and taking proper actions for preventing or mitigating risks to the critical service. Establishing a comprehensive set of data collection and analysis requirements is an essential first step.

Threats are events or conditions that could disrupt the critical service. Threats relate not just to malicious activity, but also to non-malicious situations such as equipment in need of repair (e.g., not maintained or configured properly) or impending severe weather.

To identify and establish requirements for situational awareness data collection and analysis, the organization must first identify the relevant stakeholders (both internal and external to the organization) who can contribute to the elicitation of requirements. Section II, Overview, provides some examples of data feeds used to form a COP, along with some examples of relevant stakeholders who may contribute situational awareness data or receive processed situational awareness information.

Establishing situational awareness data collection and analysis requirements is an activity that must be carried out in conjunction with the risk management process. Risk management is the foundation for eliciting situational awareness requirements and the lens through which situational awareness information is interpreted and communicated. Risk management analyses determine (and, when documented, produce risk-based specifications for) what situational awareness information is important and what information particular stakeholders need to know, and when they need to know it, to avert or handle threats to the critical service and their potential negative impacts. A very useful method for generating and validating situational awareness data collection and analysis requirements is to work backwards from risk-based specifications of the needed situational awareness information to the data feeds and data analysis capabilities needed to construct that information in an accurate, inclusive, and timely manner.

A. Identify stakeholders of the situational awareness data collection and analysis activities.

Prior to establishing the requirements for situational awareness data collection and analysis, the organization should identify the stakeholders for these activities and make them aware of their roles. Stakeholders of situational awareness data collection and analysis activities have the following responsibilities:

- collecting and analyzing situational awareness data
- defining, managing, and ensuring the effectiveness of situational awareness data collection and analysis activities
- overseeing the situational awareness data collection and analysis process
- handling situational awareness data (i.e., threat information) and the results of situational awareness data analysis (e.g., sensitive aspects of the COP) in a secure manner

Examples of situational awareness data collection and analysis stakeholders include

- critical service owners
- management
- risk management staff
- situational awareness staff
- incident management staff
- vulnerability management staff
- owners and custodians of assets that underpin the service
- critical service operations staff
- critical service maintenance staff (i.e., maintenance of assets that implement the service)
- service continuity staff
- external entities responsible for some part of the service (as vendors or service providers)
- contacts at ISACs
- contacts at external incident response teams (e.g., national and/or sector specific)
- information technology staff
- staff responsible for cybersecurity controls
- staff responsible for physical security controls
- human resources

B. Elicit, specify, and document situational awareness data collection and analysis requirements.

Once all relevant stakeholders for situational awareness data collection and analysis activities have been identified, the organization should collaborate with these stakeholders, in the context of the risk analyses conducted in the risk management process, to elicit, specify, and document a comprehensive set of requirements for situational awareness data collection and analysis. The organization should also develop requirements based on the risks identified by the risk management analyses (in collaboration with appropriate stakeholders).

See the Risk Management guide, volume 7 of this series, for more information on risk analyses.

All the requirements, both elicited and developed, should then be captured in a written requirement specifications document. These requirement specifications will guide the establishment and maintenance of an infrastructure to support situational awareness monitoring activities as well as the development of policies and procedures to collect and analyze situational awareness data. Table 5 lists some examples of the issues these requirements should address.

Table 5: Examples of Situational Awareness Data Collection and Analysis Requirements[12]

Requirement	Description
Gap Analysis of Current Data Collection and Analysis	Many different processes in the organization may be currently collecting and analyzing data, so before any type of situational awareness data collection or analysis is provided, the organization should thoroughly review existing activities and then conduct a gap analysis to identify where situational awareness activities are still needed or are not addressed adequately.
Data Repository for Situational Awareness Data	An important step toward making situational awareness more comprehensive and available is to bring together existing data already being collected and create a repository for searching and correlation. It would be useful to have a repository that provides and maintains historical data along with current information. The repository could include links to all threat and intelligence reports as well as links to vulnerability and incident summaries.
Customizable Feeds and Alerts Related to Your Region, Infrastructure, and Operating Environment	Feeds and data received are customized, and the data is fine tuned to match topics of interest or incidents and vulnerabilities related to similar infrastructures, business missions, and lines of business. For example, the organization should be able to get customized information about attacks against specific operating systems, applications, or even sectors and their specific operational technology. Another important capability would be to receive information relevant to your particular part of the world, regionally and then locally, much like the weather stations and channels provide.
Ability to Integrate Organizational Information and Correlate with Provided Feeds	The ability for an organization to take its private data and correlate it with the information provided through the external data collection would be a major benefit.
Ability to Automate Actions	This capability would allow the organization to take incoming trusted information and filter it through their established criteria to create automatic actions in their infrastructure. Such actions could include implementing blocks; adding IPs, domains, or sites to blacklists; and adding signatures for detection in intrusion detection systems (IDS) and intrusion prevention systems (IPS).
Ability to Get Feed of Known Fixes	This could also tie into the historical data in the repository.
Real-World News Feeds	This should include not only specific cybersecurity-related activity, but also social, political, economic, and regional news feeds. This information would be specifically related to ongoing critical infrastructure activities; where international organizations are meeting; where decision makers are gathering for conferences, summits, sports, or cultural activities; and similar information that can be used to provide context to received network and system activities.
Continuous Information Collection, Correlation, and Analysis	Very often, analysis of threats is only done periodically, perhaps every quarter, six months, or year. Continuous trend analysis on current threat data would be extremely beneficial, specifically, the ability to quickly understand historical and contextual information surrounding some new report.
Impact Analysis Performed	To react in a timely manner, the organization needs to know what impact threat data has (or would have) on their environment.
Root Cause Information and Long-Term Analysis Collected	Situational awareness should not only focus on current attacks, but should also strive to collect lessons learned and after-the-fact (a.k.a. “post-mortem”) analyses so that the organization can better understand what happened and how it could be stopped or prevented in the future.
A Heartbeat in the Collection of Data	Ensure freshness of data to detect adverse events and prevent “replay” attacks.

Step 2. Establish an approach to collecting and analyzing situational awareness data.

A crucial next step is to identify and implement standards for the collection and analysis of situational awareness data. First, the organization needs to identify relevant standards to form a foundation for performance requirements and expectations. The organization should then issue guidelines (typically in the

form of organizational policies and procedures) to ensure that the performance of situational awareness monitoring and analysis activities meets standards and is predictable, measurable, and repeatable.

Standards and guidelines typically address

- identification of threat monitoring requirements
- identification of threat communication requirements and protocols (e.g., whom to call and when)
- identification of threat communication methods and channels
- communications with stakeholders based on their role
- collection and storage of threat data
- distribution of threat data

NIST Special Publication 800-53 Revision 4,[13] a security and privacy standard for federal information systems, has been widely applied to industrial control systems (ICS). Its security control SI-4, "Information System Monitoring," is directly relevant to the collection and analysis of situational awareness data. In particular, SI-4 control enhancement #24 relates to the collection and use of forensic data ("indicators of compromise"):

> **The information system discovers, collects, distributes, and uses indicators of compromise.**
>
> Supplemental Guidance: Indicators of compromise (IOC) are forensic artifacts from intrusions that are identified on organizational information systems (at the host or network level). IOCs provide organizations with valuable information on objects or information systems that have been compromised. IOCs for the discovery of compromised hosts can include for example, the creation of registry key values. IOCs for network traffic include, for example, Universal Resource Locator (URL) or protocol elements that indicate malware command and control servers. The rapid distribution and adoption of IOCs can improve information security by reducing the time that information systems and organizations are vulnerable to the same exploit or attack.

Related NIST Special Publications referenced by the SI-4 control include NIST SPs 800-61,[14] 800-83,[15] 800-92,[16] 800-94,[17] and 800-137.[18] Other relevant NIST publications to consider include NIST Interagency Report (IR) 7848,[19] NIST IR 7800,[20] NIST SP 800-117 Rev. 1,[21] NIST IR 7799,[22] NIST IR 7756,[23] and NIST SP 800-155.[24]

Step 3. Establish and maintain an infrastructure to support situational awareness monitoring activities.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/ Subcategory
Goal 1: Threat monitoring is performed.	
1. Has responsibility for monitoring sources of threat information been assigned? [MON:SG1.SP1]	**ID.RA-2:** Threat and vulnerability information is received from information sharing forums and sources
	PR.AT-5: Physical and information security personnel understand roles & responsibilities
2. Have threat monitoring procedures been implemented? [MON:SG2.SP2]	**ID.RA-3:** Threats, both internal and external, are identified and documented
3. Have resources been assigned and trained to perform threat monitoring? [MON:SG2.SP3]	**PR.AT-5:** Physical and information security personnel understand roles & responsibilities

A. Assign qualified staff to perform situational awareness activities.

Once the requirements for situational awareness data collection and analysis have been developed and documented, the next step is to assign qualified staff the roles and responsibilities to perform situational awareness activities. This includes making assigned staff aware of all their responsibilities and updating job descriptions. Qualified staff are those that have the appropriate skills to perform situational awareness activities. If staff do not have necessary skills, then qualified staff must be hired or current staff members must be trained.

Responsible staff members typically include

- CISO office
- IT security personnel
- physical security personnel
- technology administrators (e.g., network, server, database)
- asset owners

Examples of staff member responsibilities include

- identification of the threat monitoring and communications requirements
- implementation of processes, standards, and guidelines
- execution of threat monitoring and communication processes
- addressing of issues and problems, including development and execution of remediation plans

Examples of needed knowledge and skills include

- knowledge necessary to elicit and prioritize stakeholder requirements and interpret them to develop effective threat monitoring and communication requirements
- knowledge necessary to establish and maintain the threat monitoring and communications infrastructure
- knowledge necessary to interpret threat information and communicate it to stakeholders
- proficiency with tools, techniques, and methods used to monitor and communicate about threats

B. Assign and train resources to perform threat monitoring.

The key requirements for this step are the following:

- The threat monitoring program must consider the scope and breadth of the activities necessary to meet its goals, including the human resources necessary to fulfill requirements.
- Staff assigned to the monitoring process must have appropriate knowledge of threat monitoring procedures.
- Training or skills improvement activities must be conducted to meet threat monitoring requirements.

Examples of training topics include

- operating, monitoring, and configuring monitoring system components
- securing data collected from monitoring system components
- understanding and interpreting monitoring data
- communicating threat monitoring information to stakeholders

C. Acquire necessary technologies.

Technologies necessary for situational awareness data collection and analysis include the following:

- reporting and alerting infrastructure
  - sensors, intrusion detection and protection systems (IDS/IDP), security information and event management (SIEM) products and services
- data repositories and logging mechanisms
- statistical analysis packages
- third-party monitoring services
- necessary licenses and access to information feeds

Step 4. Collect, record, and analyze information.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/ Subcategory
Goal 1: Threat monitoring is performed.	
2. Have threat monitoring procedures been implemented? [MON:SG2.SP2]	**ID.RA-3:** Threats, both internal and external, are identified and documented

To enable the core situational awareness activity of threat monitoring, an organization must assign responsibility for monitoring sources of threat information and establish procedures for collecting, recording, and analyzing situational awareness data.

A. Assign responsibility for monitoring sources of threat information.

Effective threat monitoring requires that the organization assign responsibility for threat monitoring activities. Threat monitoring is a process of data collection and distribution with the purpose of providing timely, accurate, complete, and relevant information about the organization's current threat environment. Threat monitoring is an integral part of establishing a COP for the organization.

B. Establish procedures for collecting, recording, and analyzing data.

Effective threat monitoring requires that the organization implement threat monitoring procedures.

- Effective monitoring requires people, procedures, and technology that need to be deployed and managed to meet monitoring requirements.
- Procedures ensure the timeliness, consistency, and accuracy of threat information and the distribution of this information to relevant stakeholders.

Procedures should address

- information source identification and prioritization
- monitoring frequency
- threat identification
- threat validation and analysis
- threat communication
- data analysis
  - impact analysis
  - trend analysis
- categorization of information (e.g., by criticality, likelihood, timeframe)
  - reporting analysis findings (this includes decisions on when to communicate threat information or declare an incident)

Example sources of threat data include

- vendors' notifications
- industry groups (e.g., Internet Storm Center, Nextgov Threatwatch)
- international sources (e.g., multinational vendors, CERT-EU)
- weather alerts (NOAA)
- law enforcement (FBI InfraGard, IC3)
- DHS (ICS-CERT, US-CERT, sector-specific ISACs)

Output of Section IV

	Output	Guidance
✓	List of stakeholders	• All internal stakeholders that need threat information have been identified and documented.
✓	List of collection and analysis requirements	• Participants in the situational awareness process, including owners of services, have participated in the development of the collection and analysis requirements.
✓	Key data collection and analysis procedures and policies	• The organization has documented procedures and policies for situational awareness data collection and analysis activities. These are written descriptions of how situational awareness activities will be conducted throughout the organization to ensure that appropriate threat information is collected and analyzed in a repeatable, reliable, timely, and secure manner.
✓	Resources are assigned authority and accountability	• The authority and accountability for collecting and analyzing threat information has been assigned to responsible resources and documented (ideally in job descriptions)
✓	Identified standards and guidelines for communications	• The organization has implemented documented standards and guidelines for performing situational awareness collection and analysis activities.

V. Communicate Information Needed to Make Appropriate Decisions

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 communicating situational awareness information.

	Input	Guidance
✓	Scoping statement	• Definition of what the situational awareness program needs to address
✓	Lists of stakeholders	• The list of stakeholders identified during the planning phase
✓	Key foundational processes	• Definitions of the risk management and asset management processes include the development of resilience requirements for the critical service and its supporting assets. These foundational processes and the resilience requirements they produce are the basis for specifying requirements that guide the communication of situational awareness information.
✓	Linkage to the other processes established	• Specifications of the interconnections and interactions among situational awareness and complementary processes so that they all work closely together to help ensure resilience
✓	Identified laws, regulations, and rules	• List of externally mandated requirements affecting the organization's communication of situational awareness information
✓	Processes for situational awareness	• Processes for situational awareness development, data collection, analysis, and communication, defined during the planning phase.

The ongoing collection and analysis of situational awareness data supports the creation of a continually updated COP of the state of the critical service in the context of its threat environment. Communicating accurate information in a timely manner to relevant stakeholders is essential for good decision making and allows stakeholders to take appropriate actions that prevent or mitigate risks to the critical service.

The manner in which the information is presented to stakeholders is another key aspect of supporting good decision making in the face of a dynamic risk environment. Using situational awareness data to support decision making involves careful consideration about what information to present, when to present it, to whom to present it, and in what form. Attempting to present all available situational awareness information to all stakeholders in a timely manner is almost always counterproductive, if not impossible. For rapid and effective decision making, different stakeholders typically need different views or slices of the COP that are customized for each class of stakeholder and consider characteristics such as the level of abstraction of the information presented, the focus and context of any alerts or alarms, the sensitivity of the information with respect to any associated security requirements (i.e., for the confidentiality, integrity, and availability of the data), and the form or format of the data (for human or machine consumption).

In particular, too much information can overload a human decision-maker (e.g., an operator interacting with a human-machine interface [HMI]) unless proper human-factors design reduces complexity through data reduction, summarization, and abstraction (e.g., using data visualization techniques to present information to human operators in a form that allows them to quickly grasp what is happening, drill down for more details on items of interest, and choose a proper course of action). When configuring urgent notifications (i.e., alerts and alarms) it is essential to avoid the classic alarm inundation problem, where a human operator might overlook critical alarms in a sea of relatively trivial alarms or ignore them (even turn them off) due to alarm fatigue. In general, the presentation of situational awareness data to human decision-makers should be carefully designed using human-factors principles. Organizations should enable their human decision-makers to quickly see the important information about the current or projected future state of the critical service in the context of its risk environment. What is important is ultimately determined by the risk strategy and the activities of the risk management process, with input from all relevant stakeholders.

The following steps describe the activities necessary for the effective communication of situational awareness information that supports appropriate decision-making to prevent or mitigate risks to the critical service.

Step 1. Establish situational awareness communications requirements.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/ Subcategory
Goal 2: The requirements for communicating threat information are established.	
1. Have internal stakeholders (such as critical service owner and incident management staff) been identified to whom threat information must be communicated? [COMM:SG1.SP1]	**PR.IP-8:** Effectiveness of protection technologies is shared with appropriate parties
2. Have external stakeholders (such as emergency management personnel, regulatory, and information sharing organizations) been identified to whom threat information must be communicated? [COMM:SG1.SP1]	**PR.IP-8:** Effectiveness of protection technologies is shared with appropriate parties **RS.CO-5:** Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness

Situational awareness information must be communicated in a timely manner to the appropriate stakeholders to allow them to make good decisions and take the proper actions to prevent or mitigate risks to the critical service. Establishing a comprehensive set of situational awareness communications requirements is an essential first step toward building, operating, and maintaining a situational awareness communications infrastructure and developing the policies, procedures, and guidelines that help ensure that relevant stakeholders have the threat information they need in time to inform their decisions and actions.

To identify and establish requirements for communicating situational awareness information, the organization must first identify the relevant stakeholders to whom situational awareness information must be communicated. It is a best practice to work in collaboration with internal and external stakeholders to identify and establish the situational awareness communications requirements. Section II, Overview, describes some examples of data feeds used to establish a COP along with some examples of relevant stakeholders who may contribute situational awareness data or receive processed situational awareness information (e.g., derived from the COP).

Identifying the relevant stakeholders to whom situational awareness information should be communicated is an activity that must be carried out in conjunction with the risk management process. Risk management analyses determine what situational awareness information is important, what level of information specific stakeholders

need to know, and when they need to know it in order to avert or handle threats to the critical service and their potential negative impacts.

A. Identify internal stakeholders to whom threat information must be communicated.

Building on the results of risk management analyses, the organization should identify internal stakeholders to whom threat information must be communicated. Internal stakeholders are identified in order to

- ensure communications about ongoing threat monitoring activities
- promote threat awareness
- ensure that the organization is performing under a COP so that decisions and actions are consistent and coordinated

Examples of internal stakeholders include

- critical service owners
- members of the incident handling team
- members of the management team (in particular, those involved in risk management)
- asset owners and service owners
- information technology staff
- senior management
- business and service continuity staff
- human resources department
- communications and public relations staff
- support functions such as legal and audit

The typical work products produced by the internal stakeholder identification step are

- list of internal stakeholders and alternates
- stakeholder contact information

B. Identify external stakeholders to whom threat information must be communicated.

Continuing to build on the results of risk management analyses, the organization should identify external stakeholders (such as emergency management personnel, regulators, and information sharing organizations) to whom threat information must be communicated. External stakeholders are identified to

- ensure that communications about ongoing threat monitoring activities reach relevant external stakeholders who can make decisions and take actions to prevent or mitigate risk
- ensure that communications about ongoing threat monitoring activities comply with notification requirements mandated by law or regulation
- promote threat awareness
- ensure that the organization and its external stakeholders are performing under a COP, so that decisions and actions are consistent and coordinated
- support collaboration among internal and external stakeholders when responding to a threat; for example, external stakeholders may have a stated role in communication plans, incident management plans, or the service continuity plans of the organization

Examples of external stakeholders include

- first responders, including law enforcement, fire, and medical
- media, including newspaper, television, radio, and internet
- customers, business partners, and upstream suppliers
- local, state, and federal emergency management

- local utilities such as power, gas, telecommunications, and water, if affected
- legal, regulatory, and governing agencies
- ISACs, typically sector-specific
- external incident response teams (e.g., national and/or sector-specific)

The typical work products produced by the external stakeholder identification step are
- list of external stakeholders and alternates
- stakeholder contact information

C. Elicit, specify, and document situational awareness communications requirements.

Once all the relevant internal and external stakeholders for situational awareness communications have been identified, the organization should collaborate with these stakeholders, in the context of the organization's risk management analyses, to elicit, specify, and document a comprehensive set of requirements for the communication of situational awareness information. The ultimate goal is to provide relevant stakeholders with timely, accurate, secure, and actionable (e.g., at an appropriate conceptual level) threat information, so that all stakeholders can collaborate effectively to prevent or reduce risks to the critical service. Some examples of the issues these requirements should address include the following:
- Who should receive each type of threat information?
- What are the time-sensitivity requirements?
- What level of detail, abstraction, and sensitivity/confidentiality should be provided based on the type of threat information and the class of stakeholder receiving the information?
- What communication channel(s) should be used (depending on the type of threat information and the type of stakeholder)?
- Under what circumstances is there a need for an acknowledgement of receipt from the stakeholder (i.e., a received receipt)?
- What is the appropriate level of security (confidentiality, integrity, availability) for each type of threat information?

Table 6 lists some examples of situational awareness communications requirements.

Table 6: Examples of Communications Requirements[12]

Requirement Title	Description
Identify Stakeholders Who Will Receive Communications	Different types of stakeholders may require different types of situational awareness communications. The types need to be determined and stakeholders categorized so they receive only the information they need.
Identify Communication Methods and Channels	Situational awareness communication methods and channels are identified for the different types and levels of information that are to be communicated.
Include Visualization of Trends and Other Situational Awareness Information	Being able to quickly visualize ongoing malicious activity and its impact can reduce analysis time and decrease response time. Finding standard ways to visualize correlated information will be a key to situational awareness success.
Include Different Levels of Information	It is important to consider what kinds of information specific types of stakeholders may need. Some may want indicators of the source of suspicious network activity (such as IP addresses and domain names), some may want detailed information on the status of physical processes, and some may want descriptions of actors and what type of malicious activity was being performed. Still others may want full-blown analysis of attacks, including root cause, while others may want ways of detecting similar attacks in the future (e.g., attack signatures). The situational awareness process should ensure that information is shared as needed at these different levels. The tools and feeds provided by the situational awareness process should be customizable based on the needs and interests of specific stakeholders and analysts. The collection and communication of situational awareness data may benefit by including a data architect in the design and implementation phases of establishing or enhancing a situational awareness infrastructure.
Categorize Threat Information for Communication	Threat information needs to be categorized so that the appropriate information is communicated to the appropriate stakeholders. Categories of threat information will most likely be based on criticality, impact, probability, and time sensitivity.
Include Information on Emerging Trends	To improve cybersecurity or oversee cybersecurity improvements, stakeholders need to know what evolutionary or revolutionary changes are being seen in attacks, technologies, mitigations, and even process improvement. Situational awareness activities should ensure this kind of information is collected, shared, and placed into the repository. The organization might develop some business scenario simulations, with which organizations and their service providers, vendors, and/or partners and collaborators can test changes they want to implement in infrastructures or processes to see how the risks and threats might increase or decrease based on emerging trends and predictive analysis.

Step 2. Establish communication standards and guidelines.

The organization needs to identify relevant standards as a foundation for establishing requirements and expectations for performance of situational awareness communication. The organization should then issue guidelines (typically in the form of organizational policies and procedures) to ensure that the performance of situational awareness communication activities meets standards and is predictable, measurable, and repeatable.

Standards and guidelines typically address

- identification of threat communication requirements and protocols (e.g., whom to call and when)
- identification of threat communication methods and channels
- communications with stakeholders based on their role
- stakeholder access to collections (i.e., repositories) of stored threat data and analyses, including trends
- security of threat data and analysis results, in transit and in storage

As an example, NIST Special Publication 800-53 Revision 4[13] contains security control SI-5, “Security Alerts, Advisories, and Directives,” which is highly relevant to the communication of situational awareness data. The description of this control also references a related publication, NIST SP 800-40.[25]

Step 3. Establish and maintain an infrastructure to support situational awareness communication activities.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/ Subcategory
Goal 3 – Threat information is communicated.	
2. Have resources been assigned authority and accountability for communicating threat information? [COMM:SG2.SP3]	**PR.AT-5:** Physical and information security personnel understand roles & responsibilities
3. Have resources been trained with respect to their specific role in communicating threat information? [COMM:SG2.SP3]	**PR.AT-1:** All users are informed and trained
	PR.AT-5: Physical and information security personnel understand roles & responsibilities

A. Establish procedures for communicating situational awareness information.

The effective communication of situational awareness information to stakeholders requires the organization to implement situational awareness communication procedures.

- Effective situational awareness communication requires people, procedures, and technology that need to be deployed and managed to meet situational awareness communication requirements.
- Procedures ensure the timeliness, consistency, accuracy, and security of situational awareness information and the distribution of this information to relevant stakeholders.

Procedures should be established to address

- categorization of information (e.g., by criticality, likelihood, timeframe)
- the manner in which critical information is to be communicated and presented (e.g., alarm strategy)
- when to communicate threat information and when to declare an incident (should be linked to procedures in the incident management process)
- establishment of procedures for communicating situational awareness information by
  - threat information category
  - recipient of the threat information
  - communication channel used
- monitoring of situational awareness communications activities and obtaining feedback from stakeholders on quality and effectiveness

B. Assign responsibility (authority and accountability) for communicating threat information.

Effective threat communication requires the organization to assign authority and accountability for threat communication activities:

- Resources must be available to meet threat communication requirements.
- The authority and accountability should be detailed in job descriptions.
- Skilled staff are assigned roles and responsibilities.
  - If staff do not have necessary skills, qualified staff should be hired or current staff should be trained.
  - Ensure assigned staff are made aware of all their responsibilities.
  - Update job descriptions of assigned staff to reflect new or changed responsibilities.

C. Train the resources responsible for communicating situational awareness information for their specific role.

The following activities will help the personnel responsible for communicating situational awareness information to effectively carry out their tasks:

- Provide training to staff that support and enable situational awareness communications procedures.
- Use a skills inventory and gap analysis to identify training requirements.

Typical work products that result from this step include

- situational awareness communication procedures with resources assigned
- job descriptions that contain threat communication responsibilities
- list of available and skilled resources
- list of skill and resource gaps
- training plan and/or hiring plan to address skill gaps

The desired outcome of this step is that all personnel assigned to perform situational awareness communication activities have been sufficiently well trained.

D. Acquire necessary technologies.

The organization must consider what technology is needed to communicate information quickly and securely to both a large audience—most or all of the internal stakeholders—and a select group—potentially, executive management or a "need to know" list for sensitive information.

External stakeholders, such as vendors and customers, are usually contacted individually, as information shared with them may differ from information shared internally. For example, a designated person in the organization calls the point of contact (POC) at an ISAC and then contacts an organizationally approved list of POCs at vendors, local authorities, and so forth. The organization may also have a media relations person responsible for contacting and interacting with news organizations.

Equipment and services typically required for communication of situational awareness information include

- communication technologies and communication service providers that provide security for data in transit
- emergency communication devices
- speed dialer products with groups and messaging to automate contacts
- Human-machine interfaces (HMIs) for the presentation of situational awareness information (and operator training packages)
- data visualization tools and packages
- secure internal data links for contacting internal stakeholders

Communication may also go through an Emergency Operations Center (EOC) and its associated infrastructure.

Step 4. Communicate situational awareness information.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/ Subcategory
Goal 3: Threat information is communicated.	
1. Is threat information communicated to stakeholders? [COMM:SG3.SP2]	**PR.IP-8:** Effectiveness of protection technologies is shared with appropriate parties
	RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness

The organization must assign responsibility and establish procedures for communicating threat information to relevant stakeholders.

A. Communicate threat information to stakeholders.

The intent of communicating threat information is to ensure that the organization is operating under a common understanding of the threat environment, and that stakeholders receive accurate and appropriate situational awareness information in a timely manner to support decisions about risks to the critical service. For organizations to enable this capability,

- threat information must be communicated according to established requirements
- communication requirements may dictate that various communications methods and channels should be considered and identified
- the infrastructure to support those methods may need to be developed and implemented

Example methods of elements that contribute to the organizational capability to communicate situational awareness information include

- situational awareness communication standards and guidelines
- standardized report templates
- standardized situational awareness communication data formats and protocols
- communication escalation protocols
- communication channels (email, text, mobile phone, emergency radio, etc.)

There are typical work products, produced in earlier steps, that should be available by the time the organization reaches this step. These products enable situational awareness communication to occur according to organizational requirements and guidelines:

- list of stakeholders and contact information
- stakeholder communication requirements
- documented methods and channels (by stakeholder type or requirement)
- tools and techniques for communication

B. Communicate emerging trends to stakeholders.

In addition to communicating threat information that is to be used by stakeholders for immediate or short-term decision-making, the organization's situational awareness process should make information available periodically to relevant stakeholders about emerging threats and other trends (e.g., technical, political, economic, legal, regulatory) that could affect risks to the critical service. This information helps relevant stakeholders make long-term strategic decisions that would reduce risks to the critical service as well as mitigate the potential impacts of such risks.

Output of Section V

	Output	Guidance
✓	List of internal stakeholders	• All internal stakeholders that receive threat information have been identified and documented.
✓	List of external stakeholders	• All external stakeholders that receive threat information have been identified and documented.
✓	List of communications requirements	• Participants in the situational awareness process, including owners of services, have participated in the development of the collection and analysis requirements.
✓	Key communications procedures and policies	• The organization has documented procedures and policies for situational awareness communication activities. These are written descriptions of how situational awareness communication activities will be conducted throughout the organization to ensure that appropriate threat information is communicated to identified stakeholders in a timely and secure manner.
✓	Resources are assigned authority and accountability	• The authority and accountability for communicating threat information has been assigned to responsible resources and documented (ideally in job descriptions).
✓	Identified standards and guidelines for communications	• The organization has implemented documented standards and guidelines for performing situational awareness communication activities.

VI. Improve Situational Awareness Processes and Technology

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 improving situational awareness processes and technology.

	Input	Guidance
✓	Situational awareness plan	The goals and objectives of the plan
✓	Tracking records and materials	Materials collected, analysis conducted, communications, and feedback on the communicated threat information
✓	Interviews with stakeholders	Stakeholders' observations about the effectiveness of the situational awareness activities

Step 1. Review overall situational awareness program effectiveness.

The organization should plan for the review of the situational awareness program while the program is in development.

Key personnel performing the review should have the following responsibilities:
- developing the review process and scope
- analyzing and assessing the situational awareness activities
- managing internal and external entities during the review process
- summarizing the review results

Stakeholders include
- owners of enterprise-level cybersecurity policies and procedures
- service or asset owners
- staff performing the situational awareness work

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

When reviewing the effectiveness of situational awareness activities, the organization should collect measures that allow the examination of three specific aspects of threat information:
- collection
- analysis
- communication

Collection of this data will require access to those who plan and administer the situational awareness activities and the staff who will participate in those activities.

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

- Threat information data collected is sufficient and adequate enough to enable robust threat information analysis and informed decision-making.
- Analysis tools and techniques allow for the translation of raw data into actionable information.
- The organization feels confident that threat information communication is effective and appropriate.
- The situational awareness activities can be improved.

Once the organization has developed a plan to collect the data needed to review the situational awareness program, it should implement the plan. Data may be collected continuously or after discrete events, such as after a disruption. But those reviewing the situational awareness activities should establish a schedule that supports the collection, consolidation, and analysis of data and enables Step 3 (Make improvements to the processes and technology).

Using the objectives that define situational awareness activities, reviewers should organize the data to support a regular review cycle. Data collected to support this analysis comes from three sources:

- the stakeholders who receive threat information communications
- corporate leadership that establishes performance objectives to accomplish the organization's mission
- those who actually perform the situational awareness activities

Examples of situational awareness process measures include

- uptime or availability of monitoring and communications infrastructure
- level of adherence to situational awareness process activities
- percentage of work products that do not meet standards
- percentage of stakeholders that do not receive communications
- time elapsed between the collection of key threat information and its distribution to stakeholders
- number of situational awareness requirements gaps
- number of new and changed situational awareness requirements over time

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

Step 2. Identify updates and improvements to the situational awareness program.

A. Identify weaknesses.

Reviewers should be looking for and documenting weaknesses such as the following:

- conditions (e.g., needed analysis tools are not available)
- ineffective training (e.g., employees are consistently unable to demonstrate needs skills to perform situational awareness activities)
- insufficient impact on organizational resilience (e.g., communications methods or channels are not appropriately used)

B. Leverage existing assessment results.

Reviews 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 situational 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. Make improvements to the processes and technology.

Situational awareness capabilities must be kept current and up to date; communicated situational awareness threat information must be effective in the eyes of the stakeholders receiving the information.

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

A. Use the feedback loop.

As depicted in Figure 1, an organization's review of its situational awareness activities is an ongoing process. As technology and processes change, so must the situational 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 situational 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 situational awareness program will become known. These gaps should be discussed during the post-incident brief, and recommendations to improve the situational 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 situational awareness activities should be fed into the situational awareness plan.
- service continuity—As disaster recovery and business continuity plans are developed and exercised, failures should be documented and recommendations for new situational awareness requirements and activities should be fed into the situational awareness program.

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

B. Implement improvements.

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

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

Output of Section VI

	Output	Guidance
✓	Review report	• Review report that outlines the areas below
✓	Review of effectiveness of communications	• As reported by stakeholders receiving the communications
✓	Return on investment	• Supports resource allocation to the most effective situational awareness activities
✓	Remediation plans	• Plans that will ensure situation awareness objectives are satisfactorily addressed

VII. Conclusion

Situational awareness involves collecting, analyzing, and communicating information that provides a broader and richer perspective of the organization's operating environment. Situational awareness maintains an ever-evolving picture of the surrounding environment in which daily activity is occurring. By including economic, social, political, and geographic events into the assessment process, events that by themselves may not seem noteworthy can be identified as suspicious or even malicious. This context in which to observe, assess, and correlate events and information is required at the local or internal organizational level (organizational events such as layoffs, special high profile events, etc.) and also at the external or national or world level (meetings of international organizations in the limelight or under scrutiny such as the World Bank, Olympics, etc.).[12]

For information on the phases an analyst goes through to perform situational awareness, to understand how mental models play a part, and to see how the data may need to be fed as part of the service, see D'Amico, Whitley, Tesone, O'Brien, and Roth (2005).[26] For more information about mental models, see Floodeen (2013).[27] Hutchins, Clopperty, and Amin (2010)[28] talk about the Lockheed Martin Kill Chain in the article *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*. It may be worthwhile to explore how information can be shared in a situational context according to how the attacks moved through the kill chain process. Doing so may yield some correlations that can identify precursors for future attacks.

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. Situational Awareness Resources

United States Computer Emergency Readiness Team (US-CERT)	US-CERT is the operational arm of the National Cybersecurity and Communications Integration Center (NCCIC) at DHS. US-CERT's mission is to improve the nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the nation while protecting the constitutional rights of Americans. **US-CERT:** http://www.us-cert.gov/ **National Cyber Alert System:** http://www.us-cert.gov/ncas
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 (http://www.nist.gov/cyberframework/). **Getting Started for Business resources:** http://www.us-cert.gov/ccubedvp/getting-started-business **Cyber Resilience Review (CRR) assessment resources:** http://www.us-cert.gov/ccubedvp/self-service-crr
Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)	ICS-CERT provides a control system security focus in collaboration with US-CERT. ICS-CERT serves as a key component of the Strategy for Securing Control Systems, which outlines a long-term, common vision where effective risk management of control systems security can be realized through successful coordination efforts. **ICS-CERT:** http://www.us-cert.gov/control_systems/ics-cert/ **CSSP Training:** http://ics-cert.us-cert.gov/sites/default/files/DHS_CyberSecurity_CSSP-Traning-v12.pdf **Cyber Security Evaluation Tool (CSET):** http://www.us-cert.gov/control_systems/satool.html
National Cybersecurity and Communications Integration Center (NCCIC)	The NCCIC is a 24x7 center responsible for the production of a common operating picture for cyber and communications across the federal, state, and local government, intelligence, and law enforcement communities, and the private sector. **NCCIC:** http://www.dhs.gov/about-national-cybersecurity-communications-integration-center
Daily Open Source Infrastructure Report	Each business day, the DHS collects a summary of open-source published information concerning significant critical infrastructure issues. **Daily Open Source Infrastructure Report:** http://www.dhs.gov/files/programs/editorial_0542.shtm
Homeland Security Information Network (HSIN)	HSIN is a national secure and trusted web-based portal for information sharing and collaboration among federal, state, local, tribal, territorial, private-sector, and international partners engaged in the homeland security mission. **HSIN:** http://www.dhs.gov/files/programs/gc_1156888108137.shtm
Multi-State Information Sharing and Analysis Center	The MS-ISAC is the focal point for cyber threat prevention, protection, response, and recovery for the nation's state, local, territorial, and tribal (SLTT) governments. http://msisac.cisecurity.org/resources/videos/free-training.cfm
United State Secret Service (USSS) Electronic Crimes Task Force (ECTF)	Partnership of not only federal, state, and local law enforcement, but also prosecutors, private industry, and academia. Its common purpose is the prevention, detection, mitigation, and aggressive investigation of attacks on the nation's financial and critical infrastructures. **USSS ECTF:** http://www.secretservice.gov/ectf.shtml
Federal Bureau of Investigation (FBI) InfraGard	InfraGard, a partnership between the FBI and the private sector, is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. **InfraGard:** http://www.infragard.net/
Internet Crime Complaint Center (IC3)	The IC3 is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C). The IC3

	provides a central point for internet crime victims to report to and alert an appropriate agency online at www.ic3.gov collects, reviews, and refers internet crime complaints to law enforcement agencies with jurisdiction to aid in preventive and investigative efforts identifies current crime trends over the internet **IC3:** http://www.ic3.gov/default.aspx
iGuardian	In its pilot stage, iGuardian portal is available to 58,000 companies that make up the FBI's InfraGard network. If the pilot succeeds, the FBI plans to open it up to more organizations, probably at first in critical infrastructure sectors. Participating companies can submit a form online in the instance of a cybersecurity breach to their networks. The National Cyber Investigative Joint Taskforce (NCI-JTF) handles the information provided by these companies. **iGuardian:** http://www.fbi.gov/news/podcasts/thisweek/iguardian.mp3/view **NCI-JTF:** http://www.fbi.gov/about-us/investigate/cyber/ncijtf

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

Table 7 cross-references the CRR Situational 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 https://www.us-cert.gov/ccubedvp also provides informative references for interpreting Category and Subcategory statements.

Table 7: Cross-Reference of CRR Goals/Practices and NIST CSF Categories/Subcategories Against the Situational Awareness Resource Guide

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/ Subcategory	Situational Awareness Resource Guide Reference
Goal 1: Threat monitoring is performed.	—	—
1. Has responsibility for monitoring sources of threat information been assigned? [MON:SG1.SP1]	**ID.RA-2:** Threat and vulnerability information is received from information sharing forums and sources **PR.AT-5:** Physical and information security personnel understand roles & responsibilities	Section IV, Step 3
2. Have threat monitoring procedures been implemented? [MON:SG2.SP2]	**ID.RA-3:** Threats, both internal and external, are identified and documented	Section IV, Step 3 Section IV, Step 4
3. Have resources been assigned and trained to perform threat monitoring? [MON:SG2.SP3]	**PR.AT-5:** Physical and information security personnel understand roles & responsibilities	Section IV, Step 3
Goal 2: The requirements for communicating threat information are established.	—	—
1. Have internal stakeholders (such as critical service owner and incident management staff) been identified to whom threat information must be communicated? [COMM:SG1.SP1]	**PR.IP-8:** Effectiveness of protection technologies is shared with appropriate parties	Section V, Step 1
2. Have external stakeholders (such as emergency management personnel, regulatory, and information sharing organizations) been identified to whom threat information must be communicated? [COMM:SG1.SP1]	**PR.IP-8:** Effectiveness of protection technologies is shared with appropriate parties **RS.CO-5:** Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	Section V, Step 1
Goal 3: Threat information is communicated.	—	—
1. Is threat information communicated to stakeholders? [COMM:SG3.SP2]	**PR.IP-8:** Effectiveness of protection technologies is shared with appropriate parties **RS.CO-5:** Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	Section V, Step 4
2. Have resources been assigned authority and accountability for communicating threat information? [COMM:SG2.SP3]	**PR.AT-5:** Physical and information security personnel understand roles & responsibilities	Section V, Step 3
3. Have resources been trained with respect to their specific role in communicating threat information? [COMM:SG2.SP3]	**PR.AT-1:** All users are informed and trained **PR.AT-5:** Physical and information security personnel understand roles & responsibilities	Section V, Step 3

Endnotes

1. For more information on the *Cyber Resilience Review*, please email the Cyber Security Evaluation Program at CSE@hq.dhs.gov
2. The *CERT-RMM* (Glossary of Terms) [Caralli 2010]
3. Caralli, R. A.; Allen, J. A.; & White, D. W. *CERT® Resilience Management Model: 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. Department of Homeland Security. *Cyber Resilience Review (CRR): Method Description and Self-Assessment User Guide*. Carnegie Mellon University, 2014. http://www.us-cert.gov/sites/default/files/c3vp/csc-crr-method-description-and-user-guide.pdf
5. Endsley, M.R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors 37*(1), 32–64.
6. The *CERT-RMM* (EF:SG1) [Caralli 2010] discusses the need for resilience activities to meet strategic objectives.
7. Gates, L. P., *Strategic Planning with Critical Success Factors and Future Scenarios: An Integrated Strategic Planning Framework* [CERT 2010] discusses strategic planning.
8. Gates, L. P., *Strategic Planning with Critical Success Factors and Future Scenarios: An Integrated Strategic Planning Framework* [CERT 2010] discusses strategic planning.
9. The *CERT-RMM* (OTA:SG1and SG3) [Caralli 2010] discusses how to identify management directives and organizational guidelines.
10. The *CERT-RMM* (OTA:SG1and SG3) [Caralli 2010] discusses how to identify management directives and organizational guidelines.
11. The *CERT-RMM* (OTA:SG1:SP1and SG3:SP1) [Caralli 2010] discusses prioritizing objectives.
12. Software Engineering Institute, Carnegie Mellon University. *CSIRT Requirements for Situational Awareness Tools*. Unpublished white paper.
13. National Institute of Standards and Technology (NIST), U.S. Department of Commerce. *NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations*. NIST, 2014. http://www.nist.gov/manuscript-publication-search.cfm?pub_id=915447
14. National Institute of Standards and Technology (NIST), U.S. Department of Commerce. *NIST Special Publication 800-61 Revision 2, Computer Security Incident Handling Guide*. NIST, 2012. http://www.nist.gov/manuscript-publication-search.cfm?pub_id=911736
15. National Institute of Standards and Technology (NIST), U.S. Department of Commerce. *NIST Special Publication 800-83 Revision 1, Guide to Malware Incident Prevention and Handling for Desktops and Laptops*. NIST, 2013. http://www.nist.gov/manuscript-publication-search.cfm?pub_id=913930
16. National Institute of Standards and Technology (NIST), U.S. Department of Commerce. *NIST Special Publication 800-92, Guide to Computer Security Log Management*. NIST, 2006. http://www.nist.gov/manuscript-publication-search.cfm?pub_id=50881

17. National Institute of Standards and Technology (NIST), U.S. Department of Commerce. *NIST Special Publication 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS) (Revision 1, Draft)*. NIST, 2012. http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-94-Rev.%201

18. National Institute of Standards and Technology (NIST), U.S. Department of Commerce. *NIST Special Publication 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*. NIST, 2011. http://www.nist.gov/manuscript-publication-search.cfm?pub_id=909726

19. National Institute of Standards and Technology (NIST), U.S. Department of Commerce. *NIST Interagency Report 7848, Specification for the Asset Summary Reporting Format 1.0 (Draft)*. NIST, 2012. http://csrc.nist.gov/publications/PubsDrafts.html#NIST-IR-7848

20. National Institute of Standards and Technology (NIST), U.S. Department of Commerce. *NIST Interagency Report 7800, Applying the Continuous Monitoring Technical Reference Model to the Asset, Configuration, and Vulnerability Management Domains (Draft)*. NIST, 2012. http://csrc.nist.gov/publications/PubsDrafts.html#NIST-IR-7800

21. National Institute of Standards and Technology (NIST), U.S. Department of Commerce. *NIST Special Publication 800-117 Revision 1, Guide to Adopting and Using the Security Content Automation Protocol (SCAP) Version 1.2 (Draft)*. NIST, 2012. http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-117-Rev.%201

22. National Institute of Standards and Technology (NIST), U.S. Department of Commerce. *NIST Interagency Report 7799, Continuous Monitoring Reference Model Workflow, Subsystem, and Interface Specifications (Draft)*. NIST, 2012. http://csrc.nist.gov/publications/PubsDrafts.html#NIST-IR-7799

23. National Institute of Standards and Technology (NIST), U.S. Department of Commerce. *NIST Interagency Report 7756, CAESARS Framework Extension: An Enterprise Continuous Monitoring Technical Reference Architecture (Draft)*. NIST, 2012. http://csrc.nist.gov/publications/PubsDrafts.html#NIST-IR-7756

24. National Institute of Standards and Technology (NIST), U.S. Department of Commerce. *NIST Special Publication 800-155, BIOS Integrity Measurement Guidelines (Draft)*. NIST, 2011. http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-155

25. National Institute of Standards and Technology (NIST), U.S. Department of Commerce. *NIST Special Publication 800-40, Guide to Enterprise Patch Management Technologies*. NIST, 2013. http://www.nist.gov/manuscript-publication-search.cfm?pub_id=913929

26. D'Amico, Anita; Whitley, Kirsten; Tesone, Daniel; O'Brien, Brianne; & Roth, Emilie. "Achieving Cyber Defense Situational Awareness: A Cognitive Task Analysis of Information Assurance Analysts," 229-233. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 49*, 3 (2005). Orlando, FL, Sep. 2005. Sage, 2005. http://pro.sagepub.com/content/49/3/229

27. Floodeen, Robert; Haller, John; & Tjaden, Brett. "Identifying a Shared Mental Model Among Incident Responders,"15-25. *2013 Seventh International Conference on IT Security Incident Management and IT Forensics*. Nuremberg, Germany, Mar. 2013. IEEE, 2013. http://www.computer.org/csdl/proceedings/imf/2013/4955/00/4955a015-abs.html

28. Hutchins, Eric M.; Clopperty, Michael J.; & Amin, Rohan M. *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*. Lockheed Martin, 2010. http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf