Carnegie Mellon University
Software Engineering Institute

Incident Management Capability Assessment

Audrey Dorofee
Robin Ruefle
Mark Zajicek
David McIntire
Christopher Alberts
Samuel Perl
Carly Lauren Huth
Pennie Walters

December 2018

TECHNICAL REPORT

CMU/SEI-2018-TR-007

CERT Division

This document supersedes Version 0.1 of the *Incident Management Capability Metrics* published in 2007 as CMU/SEI-2007-TR-008.

http://www.sei.cmu.edu

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

This report was prepared for the SEI Administrative Agent AFLCMC/AZS 5 Eglin Street Hanscom AFB, MA 01731-2100

DM18-0962

Table of Contents

Abstract

Successful management of incidents that threaten an organization's computer security is a complex endeavor. Frequently an organization's primary focus is on the response aspects of security incidents, which results in its failure to manage incidents beyond simply reacting to threatening events.

The capabilities presented in this document are intended to provide a baseline or benchmark of incident management practices for an organization. The incident management capabilities—provided in a series of statements and indicators—define the actual benchmark. The capabilities explore different aspects of incident management activities for preparing or establishing an incident management function; protecting, detecting, and responding to unauthorized activity in an organization's information systems and computer networks; and sustaining the ability to provide those services. This benchmark can be used by an organization to assess its current incident management function for the purpose of process improvement. This assessment will also help assure system owners, data owners, and operators that their incident management services are being delivered with a high standard of quality and success within acceptable levels of risk.

1 Introduction

1.1 About This Report: A Benchmark

The Software Engineering Institute (SEI) is publishing this method to be used to proactively evaluate and improve an organization's or department's ability to manage computer security incidents. It is not intended for more than process improvement. This method cannot measure how well a given incident management activity is performed, only that it is performed.

This set of incident management capabilities[1] has evolved over many years. It is based on a set of metrics developed by the Defense Information Systems Agency (DISA) and National Security Agency (NSA) in 2000-2002 and called the *DoD Computer Network Defense Service Provider (CNDSP) "Evaluator's Scoring Metrics."* The Department of Homeland Security (DHS) and United States Computer Emergency Readiness Team (US-CERT) funded initial work to adapt the U.S. Department of Defense (DoD) version for Federal use in 2003–2005. As a result, the Federal-Computer Network Defense (F-CND) metrics were piloted with multiple agencies in 2006 and published in limited distribution under the title *Federal Metrics*. In 2007 a generic or public version of this assessment instrument was published on the CERT web page as the Incident Management Capability Metrics.[2]

During 2011–2013 the F-CND assessment was updated to align it with the DHS Cybersecurity Capability Validation (CCV) suite of products. As part of the realignment, the Federal Metrics were renamed F-CND Capabilities. This current SEI Technical Report, *Incident Management Capability Assessment*, is the public, generic version of the updated F-CND capabilities. The capabilities can be used as a stand-alone assessment or to provide a deeper assessment of the incident management aspects of an organization's security program and processes. The assessment method is summarized in Sections 3 and 4.

There are many aspects to successfully managing computer security incidents within an organization. Frequently, the primary focus is on the response aspects of computer security incidents. As a result, the organization fails to adequately consider that there is more to incident management than just responding when a threatening event occurs.

The capabilities in this document provide a baseline or benchmark of incident management practices. The incident management capabilities—each including a series of indicators—define the actual benchmark.

This benchmark can be used by organizations to assess how their current incident management functions are defined, managed, and measured. This provides the basis for improvements to the incident management function.

---

[1] A capability can be considered to be the people, processes, technology, and so forth that provide an ability or capacity to perform some task.

[2] All references to Federal issues are removed from clarification and indicators. However, all references to Federal documents and guidance are still included, along with references to non-Federal—including international, legal, and policy—guidance.

1.2 Intended Audience

This report is intended for individuals and organizations that want to baseline their incident management functions to identify strengths and weaknesses and improve their incident management function. Guidance is provided to help individual practitioners or assessment teams understand how to apply these capabilities and indicators to gain an understanding of the effectiveness of their incident management function.

1.3 What Are These Capabilities?

As previously mentioned, these capabilities can be used to benchmark or evaluate an incident management function.[3] In an organization, one or more groups may be involved in incident management. Each group has a set of its own goals, tasks, and activities (i.e., the group's mission) that must be completed to support the overall strategic mission of the organization. The capabilities in this report explore different aspects of incident management activities for protecting, detecting, and responding to unauthorized activity in an organization's information systems and computer networks, as well as for establishing and sustaining the ability to provide those services.

Each capability includes a set of indicators, which are used by an assessment team to determine whether a capability has successfully been achieved or met. The results from an assessment can help an organization determine the comprehensiveness of its incident management function.

A complete list of just the capability statements is provided in Appendix A.

1.4 What We Mean by Incident Management Function (IMF)

An *incident management function* is a set of capabilities (the people, processes, technology, etc. that provide an ability or capacity to perform some task) considered essential to protecting, detecting, and responding to incidents, as well as sustaining the incident management function (refer to Alberts and colleagues for more information [Alberts 2004]). These capabilities can be provided internally by security or network operators; be outsourced to managed security service providers (MSSPs); or be provided and managed by a computer security incident response team (CSIRT), security operations center (SOC), or security team. We recognize that CSIRTs might not always be providing these capabilities.

For the sake of simplicity, the term *incident management personnel* is generally used in this report to refer to the groups (or individuals) performing incident management capabilities. The term *incident management function* includes everyone who is involved in the performance of incident management activities or the incident management process. The term *constituency* is used to refer to those who receive the services provided by whoever is performing incident management activities. The term *organization* is used to refer to the entire group that is composed of the incident management personnel as well as their constituency. Occasionally we use the term

[3] Previously, we called this an *incident management capability*. However, changing the name of the 61 metrics to capabilities made that term confusing. So we now call the performance of the incident management activities or process an *incident management function*.

CSIRT, which refers to a designated function or group of people established as a particular type of organization to perform a portion of the incident management functions.

Incident management capabilities are grouped into the five categories described in Table 1—Prepare, Protect, Detect, Respond, and Sustain. Each category contains a range of subcategories with a set of one or more capabilities. Each capability includes a set of indicators that describe the essential activities leading to adequate performance of that capability.

Within the five major categories and many subcategories, each capability is assigned a priority. These priorities can be useful when making decisions about where to focus improvement efforts.

- Priority I capabilities are critical services that an incident management function must provide.
- Priority II capabilities are important services that should be provided.
- Priority III constitutes the remaining capabilities. They represent additional best practices that enhance operational effectiveness and quality.

Table 1: Categories and Subcategories

PREPARE	PROTECT	DETECT	RESPOND	SUSTAIN
• Establish IM Function • Core Processes and Tools	• Risk Assessment • Prevention • Operational Exercises for Incident Management • Training and Guidance • Vulnerability Management	• Network and Systems Security Monitoring • Threat and Situational Awareness	• Incident Reporting • Analysis • Incident Response	• MOUs[4] and Contracts • Project/Program Management • IM Technology Development, Evaluation, and Implementation • Personnel • Security Administration • IM Information Systems

1.5 Overview of the Major Categories

The next few paragraphs provide an overview of the major categories: Prepare, Protect, Detect, Respond, and Sustain.

1.5.1 Prepare

Prepare focuses on establishing an effective, high-quality incident management function. This includes formally recognizing an incident management function, defining roles and responsibilities, and establishing interfaces between the various groups and individuals performing or affected by incident management functions. High-level processes must be defined, and essential tools, such as an incident tracking system, need to be acquired and put in place.

[4] Memoranda of Understanding

Trusted relationships, both internal and external, must be established for sharing relevant and needed information.

1.5.2 Protect

Protect relates to actions taken to prevent attacks from happening and mitigate the impact of those that do occur.

Preventative actions secure and fortify systems and networks, which helps to decrease the potential for successful attacks against the organization's infrastructure. In this model, Protect is focused on what changes can be made to the infrastructure as part of the response to contain or eradicate the malicious activity. It also includes taking proactive steps to look for weaknesses and vulnerabilities in the organization while understanding new threats and risks. Such steps can include

- performing security audits, vulnerability assessments, and other infrastructure evaluations to identify and address any weaknesses or exposures before they are successfully exploited
- collecting information on new risks and threats and evaluating their impact on the organization

Mitigation involves making changes in the constituent infrastructure to contain, eradicate, or fix actual or potential malicious activity. Such actions might include

- making changes in filters on firewalls, routers, or mail servers to prohibit malicious packets from entering the infrastructure
- updating intrusion-detection system (IDS) or anti-virus (AV) signatures to identify and contain new threats
- installing patches for vulnerable software

Changes to the infrastructure may also be made, based on the process improvement changes and lessons learned that result from a postmortem review done after an incident is handled. These types of changes are made to ensure that incidents do not happen again or that similar incidents do not occur.

1.5.3 Detect

In Detect, information about current events, potential incidents, vulnerabilities, or other computer security or incident management information is gathered both proactively and reactively. In reactive detection, information is received from internal or external sources in the form of reports or notifications. Proactive detection requires actions by the designated staff to identify suspicious activity through monitoring and analysis of a variety of logging results, situational awareness, and evaluation of warnings about situations that can adversely affect the organization's successful operation.

1.5.4 Respond

Respond includes the steps taken to analyze, resolve, or mitigate an event or incident. Such actions are targeted at understanding what has happened and what needs to be done to enable the organization to resume operation as soon as possible or to continue to operate while dealing with threats, attacks, and vulnerabilities. Respond steps can include

- analysis of incident impact, scope, and trends

- collection of computer forensics evidence, following chain-of-custody practices
- additional technical analysis related to malicious code or computer forensics analysis
- notification to constituents, stakeholders, and other involved parties of incident status and corresponding response steps
- development and release of alerts, advisories, bulletins, or other technical documents
- coordination of response actions across the organization and with other involved internal and external parties
- verification and follow-up to ensure that response actions were correctly implemented and that the incident has been appropriately handled or contained

1.5.5 Sustain

Sustain focuses on maintaining and improving the CSIRT or incident management function itself. It involves ensuring that

- the incident management function is appropriately funded
- incident management personnel are appropriately trained
- infrastructure and equipment are adequate to support the incident management services and mission
- appropriate controls, guidelines, and regulatory requirements are followed to securely maintain, update, and monitor the infrastructure
- information and lessons learned from the Protect, Detect, and Respond processes are identified and analyzed to help determine improvements for the incident management operational processes

2 Explanation of the Capability Structure

The capabilities are formatted in a workbook structure that can be used during an assessment to both conduct the assessment and capture information. The structure for each incident management capability provides two basic sets of information:

- the capability itself, presented as a primary capability statement, and a more detailed set of indicators that can be used by the assessor to assess the performance of the capability
- explanatory information and scoring guidance—additional information explaining the significance of the capability and how to assess the performance of that capability

Each capability also includes a set of cross-references to selected regulations or guidance: the Federal Information Security Management Act (FISMA), National Institute of Standards and Technology (NIST) publications, and relevant best practices.

As stated previously, each capability includes indicators to assess the performance of that capability. Within these indicators, when the word *personnel* is used, it refers to whomever is performing the activities associated with the capability. If other roles or more specific types of roles are being referenced, the indicator will specify which type of personnel.

These indicators are grouped into three areas: Required, Recommended Best Practice, and Institutional and Quality Improvement. All of the indicators in the Required area must be met for an organization to successfully meet this capability. The indicators in the Recommended Best Practice area represent additional aspects that are recommended for a more complete or robust capability. The indicators in the Institutional and Quality Improvement area are those needed to ensure this capability can be sustained, that is, those things that would ensure the continuity or resilience of the capability even in the face of personnel changes. In addition, there are four types of indicators, specified by the italicized word occurring before the indicator statement:

- *Prerequisites* must be met before this capability can be performed or be performed adequately.
- *Controls* are available or exist that direct the proper execution of the activities.
- *Activities* are performed as part of this capability (and could be observed by an assessor).
- *Quality* indicators measure effectiveness, completeness, usefulness, institutionalization, and other quality aspects of the activities.

An example of a capability table is shown in Figure 1. To help the assessor use the tables, the following list explains how the information for each capability is organized. Reading the table from left to right, the fields are

- capability subcategory and number (e.g., 2.1 Risk Assessment)
- capability reference number and statement—represents major category number, subcategory number, and specific capability number and statement (e.g., 2.1.1 Security risk assessments (RAs) are performed on the organization.)
- priority—I through III (where priority I is the most important)
- clarification—additional information explaining the purpose and description of the capability
- team guidance—information to help an assessment team score this capability

- references—standards, guidelines, or regulations relating to this capability, including a placeholder for organization-specific references
- organization response—optional field if early information was collected from an organization indicating how they would respond to the capability
- examples of evidence—list of possible evidence the team should look for during interviews, documentation reviews, or observations
- scoring criteria—the indicators (preceded by a unique indicator number), scoring choices (Yes/No), and room to list evidence (i.e., the specific criteria the assessors can see or examine during the assessment to help them determine whether the capability is being performed)
- final score—"Met" if all required indicators are met; "Not Met" if any required indicator is not met
  - Not Applicable—used when capability is excluded from scoring
  - Not Observed—used when capability was not observed during the assessment
- evidence collected—place to identify what documents were reviewed, interviews conducted, or activities observed
- notes—additional notes made by the assessment team either in preparation for the assessment or during the assessment
- suggestions for improvement—additional ideas for an organization to consider if it works to improve this particular capability beyond implementing the concepts in each indicator

X.X SUB-CATEGORY

X.X.X Capability Statement	Priority N

Clarification

Additional information to explain what the capability means

Team Guidance

Additional information to help an assessment team assess this capability

References

Regulatory and guidance references associated with this capability

Organization Response

Place to document any initial response from the organization being assessed

Examples of Evidence Sought

- ❑ Items that can be viewed as evidence that the capability is performed

Scoring Criteria	Yes	No	Evidence
Required			
x.x.x.01 Prerequisite: indicator	❒	❒	
x.x.x.02 Control: indicator	❒	❒	
x.x.x.03 Activity: indicator	❒	❒	
Recommended Best Practices			
x.x.x.04 Control: indicator	❒	❒	
x.x.x.05 Activity: indicator	❒	❒	
Institutional and Quality Improvement			
x.x.x.06 Control: indicator	❒	❒	
x.x.x.07 Quality: indicator	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒	
Not Applicable		❒	**Not Observed**	❒	
Evidence Collected					
Document Review		Interviews		Direct Observation	
Notes					
Suggestions for Improvement					
• Suggestions for additional improvements the organization can make					

Figure 1: Standard Format for an Incident Management Capability.

3 Using These Capabilities to Assess the Incident Management Function of an Organization

This section provides an overview of how the capabilities can be used to assess and improve an organization's incident management function. This section and the next provide an overview of the assessment methodology and considerations for scoring the capabilities. To generalize, this assessment method centers around using interviews, artifact reviews, and activity observations to determine how completely the incident management activities represented in the capabilities are performed.

It is possible to use these capabilities for a broad range of assessments. For example, the entire set of capabilities can be used to assess an organization's entire incident management function. A subset can be used to focus on only the specific responsibilities of an actual SOC, CSIRT, or security service provider. The extent or scope of an assessment is determined early in the process, based on the goals of the organization or the specific focus of the assessment sponsor. The assumption for this section is that the entire incident management function is being assessed. An assessment with a narrower scope would simply use fewer capabilities and assess fewer groups.

Incident management, as a complete function, includes activities that may be performed within a SOC, by a CSIRT, or by other groups across an organization. There may be several groups, each with some distinct or overlapping responsibilities that support management of cybersecurity events and incidents. In the latter case, applying these capabilities against only a designated centralized incident management function or CSIRT may result in an inaccurate or very limited view of the organization's total ability to effectively manage cybersecurity incidents. An assessment should consider all groups performing incident management activities to produce accurate results.

An assessment using these capabilities generally requires

- **assessment planning:** establishing points of contact, assessment scope, schedule, and resources and assembling the assessment team and supporting equipment and supplies
- **pre-assessment:** preparing for on-site assessment activities; gathering information as needed before going onsite; analyzing available documents and other artifacts; identifying groups and individuals (e.g., groups involved in Prepare, Protect, Detect, Respond, and Sustain activities) to interview onsite; allocating capabilities to those groups; and finalizing the onsite schedule
- **onsite:** conducting interviews, observing activities, reviewing additional artifacts, documenting evidence collected, determining preliminary scores according to evidence rules, and gathering additional information, if possible, to fill any gaps
- **post-assessment:** performing final analysis and scoring and, optionally, identifying recommendations for improvement, producing a report for stakeholders, and conducting required reviews
- **close-out:** properly disposing or archiving of gathered information and conducting a "lessons learned" review

Some specific guidance for selecting assessment activities follows.

3.1 Identify the Groups Involved in Incident Management and Allocate the Capabilities

There are many techniques for identifying the groups involved in incident management. One technique uses a process model benchmark for incident management, such as that described by Alberts and colleagues [Alberts 2004]. By comparing the organization to this process model of incident management activities, all groups performing such activities can be identified. An alternative is to use some form of work process modeling [Sharp 2001] to map all groups and interfaces associated with incident management activities. Once the groups and activities are identified, capabilities can then be allocated to each group (e.g., allocate Detect capabilities to the groups performing network monitoring).

Keep in mind that there may not be clearly defined roles that align with the categories and you may need to ask more than one group about the same set of capabilities to achieve complete coverage. While you can adjust your schedule of interviews and observations when onsite, it is best to keep schedule adjustments to a minimum.

3.2 Assess Each Group

The simplest means of assessing each group against its capabilities is to conduct interviews or group discussions, observe the activity being performed or a demonstration of the activity, and ask the assembled individuals about each capability that is applicable to their group. Artifacts related to the capabilities can be requested and reviewed and, when necessary, additional activities can be observed. The assessment team should use the general scoring guidance in Section 4 and the specific guidance provided with each capability to guide its assessment. (See Section 2, "Explanation of the Capability Structure," for a description of the sections and indicators provided for each capability.)

When more than one group shares the responsibilities to perform a certain capability, the assessment team should conduct interviews (or group discussions, observations, or process demonstrations, as applicable) with at least two of the involved groups, and then compare and assess the collective results from the different sources. (See Section 3.3 for further guidance about groups that cannot be assessed.) When the results for capabilities or individual indicators differ between groups, the lowest score generally prevails (i.e., if one individual or group indicates "Yes" to an indicator but another individual or group says "No," the combined score for the organization as a whole for that indicator will generally be "No").

All indicators are scored as either Yes or No, and Capabilities are scored at the end as "Met," "Not Met," "Not Observed," or "Not Applicable."

- "Met"—At a minimum, all of the required indicators have been met.
- "Not Met"—One or more of the required indicators has not been met.
- "Not Observed"—A capability cannot be assessed because the assessment team does not have access to the individuals who can provide the correct answer or cannot observe that the activity or capability was performed.
- "Not Applicable"—The activity is not included in the assessment, which may mean that it is deliberately not performed by the organization as part of the incident management processes. Capabilities that are not applicable should be identified during assessment scoping.

3.3 Determine What to Do About Groups That Cannot Be Assessed

Given the complexities and political realities of some organizations, it may not be possible to meet with some groups or obtain access to certain types of information. At the very least, the interface to that group or the way in which those groups interact should be assessed. The organization can then decide if those groups should be assessed at a later time. Alternatively, those groups could assess themselves using applicable information from these capabilities and then provide the results (or feedback) to appropriate individuals. Another option is to use an external or third-party organization to perform the assessment on relevant groups. If part of the incident management function is outsourced and the organization being assessed can provide sufficient evidence to prove that the outsourced contractor or group is performing the capability, the outsourced contractor or group may not need to be assessed. If specific information cannot be reviewed, the assessment team and assessment sponsor will need to decide if the remaining evidence is sufficient to indicate an actual score or if "Not Observed" needs to be used.

3.4 Use the Results to Decide What to Improve

The organization, using the assessment results, has a clear idea of how it is meeting these capabilities with respect to incident management. It knows what its strengths and weaknesses are. To improve the processes, the organization can look at the resulting scores and begin to create a strategy for improvement building on its strengths. For example, the candidates for improvement could be sorted by priority order, so that unmet Priority I capabilities come first, and so on.

Existing strengths can be used to improve weaker areas. For example, if some capabilities have exceptionally good procedures and policies, use those as a basis for developing policies and procedures for capabilities that are not as robust or are missing. If there is a strong training program for some types of personnel, expand that program to include additional types of training for capabilities that are lacking.

A further review of results may be needed when considering improvements in Priority II through Priority III capabilities. For example, improving a Priority III capability from "Not Met" to "Met" might be less critical than improving a Priority II capability from "Not Met" to "Met." Each organization makes its own determination concerning the order in which to improve scores on any Priority II-III capabilities based on a review of the entire set and by considering the changes that are needed, the required resources, the mission, the goals, and the objectives.

Finally, a common type of improvement for all the capabilities can be found by looking at the non-required indicators: Recommended Best Practices and Institutional and Quality Improvement indicators. These types of improvements go beyond meeting the basic requirements and consider additional aspects that can build an exceptional incident management function. Even those capabilities for which required indicators were successfully met can be improved by implementing the non-required indicators.

Each capability should be examined to consider the relative consequences of "doing" or "not doing" the capability or required indicators therein. This examination can provide elemental insight into whether improvement might yield an unexpected result. Look to the suggested improvements for ideas on enhancing performance or identifying ways to improve. When applying the capabilities to identify improvements, use judgment and common sense, respect the

budgetary process, and stay abreast of changing regulations and standards in this ever-evolving environment.

Ultimately, the end goal for these capabilities (or other types of assessments) is to strive for continuous improvement of the processes, so it is also a recommended best practice to periodically re-assess to see what new "current" state has been achieved. This re-assessment could be done annually or as conditions change (e.g., as new technologies are deployed, the infrastructure changes, or new partnerships or supply chains are adopted).

These capabilities should be considered a starting place for identifying improvements. They are not a precisely defined path for every organization to build the perfect incident management function, but they can be used as a guideline for what to include in an incident management function, based on the organization's mission and the incident management function's services.

4 General Guidance for Scoring Capabilities

This section discusses scoring issues that the assessment team needs to remember as it is conducting an assessment. Each capability can have a score of "Met" or "Not Met." To determine the score for a capability, the assessment team applies the rules of evidence against all the information gathered from interviews, demonstrations, observations, and document or artifact reviews. *Interviews* are question-and-answer sessions with one or more people with peer relationships where the assessment team uses the capabilities as the basis for asking questions. In *observations*, the assessment team watches one or more people conduct their actual IM activities; the team observes only and does not question or ask for additional actions. In *demonstrations*, the assessment team interacts with the people performing real or hypothetical IM activities, asking questions, getting demonstrations of what could occur, or how tools might be used in hypothetical situations. Observations and interviews are considered to be similar. *Document or artifact reviews* are conducted by assessment team members to understand relevant parts of IM-related documents.

For each capability, all Required indicators must have an answer of "Yes" to obtain a successful or passing score for that capability (i.e., the capability is met). If one or more of the Required indicators has an answer of "No," the score for the capability is "Not Met." The Recommended Best Practice indicators and the Institutional and Quality Improvement indicators include those that are not necessarily required to achieve success for the capability but are recommended. These indicators are not included in the final determination of a capability being met or not met. They are currently provided for improvement purposes. See Section 4.3 for alternative scoring ideas.

4.1 Evidence Collection Requirements

Sufficient evidence for establishing a passing score requires more than one document, interview, observation, or demonstration. The indicators listed with each capability are used to assist in the collection of evidence. The Evidence column to the right of each indicator is used to record the type of evidence (e.g., interview, observation, demonstration, or document review) or a description of the evidence that was used to score that indicator.

If a capability is to be scored "Met," all Required indicators for that capability have been determined to be covered (checked "Yes"). The coverage rules for sufficiency of evidence in order to determine if an indicator can be checked "Yes" are provided in Table 2 below. In summary, it takes at least two different types of sources to confirm an indicator. Note that in the rules for sufficiency, an interview and a demonstration are considered equivalent. An observation, then, needs the confirmation of an interview or demonstration, or a document review. A document review needs the confirmation from either an observation or a demonstration/interview. Also note that it takes at least one document, but in general, more than one document is preferred.

Table 2: Evidence Rules

	Interview/ Demonstration	**Observation**	**Document/Artifact**
Interview/ Demonstration	Not Sufficient	√	√
Observation	√	Not Sufficient	√
Document/Artifact	√	√	Not Sufficient

4.2 Check Completeness and Quality of Documented Policies and Procedures

When deciding if documented policies and procedures referenced in the indicators are adequate, assessment teams should consider the following:

- Does the policy or procedure adequately address the process, technology, requirements, expected behaviors, or other topic it is supposed to address?
- Do the procedures reflect what is actually done by personnel?
- Are the policies and procedures easily available to personnel?
- Are the policies or procedures being kept up to date? There should be a review and/or revision date or some indication that policies and procedures are reviewed and changed as needed. Also look for
  - a defined process and periodicity for reviewing and revising
  - established criteria for when to review (e.g., change in organization structure, major technology installation)
  - defined roles and responsibilities for review and update
  - a defined process for communicating changes and revisions throughout relevant parts of the organization
  - a change log history
  - indications the date was simply changed to make it look up to date[5]

It may also be useful to ask for any documents that are currently being revised to help evaluate their process for keeping documents up to date or to at least demonstrate that they are in the process of improving a current gap. Such findings will be useful when the organization decides what to improve. In most cases, policies (and processes) are included in the Required indicators, and documented, formal procedures are included in the Institutional and Quality Improvement indicators.

[5] The assessment team should use its judgment to determine if a real revision was made or if the date was simply changed to make it look up to date. The assessment team could ask to see specific changes or compare the document to the previous version to make such a determination.

4.3 Determine Personnel Knowledge of Procedures and Successful Training

The assessment team should be able to determine from discussions with the personnel whether they understand the process (e.g., they are able to intelligently and consistently describe it). More importantly, the personnel should be able to easily show how they perform that work (e.g., show the forms that they fill in, describe the process they use to take information from an incident report that is displayed and extract information to feed into summary or other organizational or regulatory reports, or demonstrate how they perform analysis on a set of logs). A process can be consistently known and followed even without a formal, documented procedure. If a documented procedure does exist, the assessment team needs to determine if the procedure is actually followed.

Training can range from formal training that has complete packages with materials and dedicated instructors to informal, on-the-job mentoring by more senior, experienced personnel. The assessment team seeks to determine whether training is provided, that the training is sufficient to meet the needs of the organization, and, as shown in the Institutional and Quality Improvement indicators, that the personnel are knowledgeable and perform the procedures consistently.

During demonstrations, the assessment team can ask personnel to discuss the process they are following to show a level of understanding that supports knowledge of their capabilities with regard to the activities being conducted. The observation of personnel performing tasks can also provide an indication of the maturity of their operations and training. For example, observation can show that personnel know the following:

- how to use the tools that support the capabilities
- where reports or data are archived
- what types of information are contained in reports or alerts or other documents and products
- where procedures, policy, or guidance documents are kept and how to access them if needed

4.4 Scoring Variations

It is possible for the assessment team and assessment sponsors to determine a different scoring algorithm (e.g., all of the Required and Recommended Best Practice for a “Met” score). The only caution would be to use a consistent scoring algorithm over time to allow for accurate determination of improvement from one assessment to the next or for accurate comparison between assessed groups.

In addition to the “Met,” “Not Met,” “Not Observed,” or “Not Applicable” scores for a capability, some assessors have used a “Partial” score. “Partial” in this case would mean that some of the Required indicators have been met, but not all. “Partial” scores can be difficult to use as it becomes more subjective as to what percentage or number of Required indicators is needed to reach a “Partial” as opposed to a “Not Met” score. Some assessment teams have also found it useful to use “Not Observed,” or “Not Applicable” for the indicators as well as the capability. In that case, on the worksheet, the indicator can be scored as either a “No,” and the evidence column used to state the rationale for it being not observed, or scored as a “Yes,” with the rationale for it not being applicable in the evidence column.

5 The Incident Management Capabilities

The remainder of this document contains Version 3.0 of the capabilities, split into five sections:

- Prepare: Section 1 of the capabilities
- Protect: Section 2 of the capabilities
- Detect: Section 3 of the capabilities
- Respond: Section 4 of the capabilities
- Sustain: Section 5 of the capabilities

These capabilities are a living document. Periodic changes may be made to these capabilities, and new versions may be released.

PREPARE: SECTION 1 OF INCIDENT MANAGEMENT CAPABILITIES

Prepare is getting the incident management function up and operational. This includes getting the incident management function established, creating and implementing the necessary plans, defining the key work processes that will be essential to the smooth functioning of an incident management function, and establishing the necessary working relationships with both internal and external experts and groups who will provide needed assistance and expertise.

Getting formal recognition and designation as an incident management function, regardless of whether it is a formal CSIRT, is essential to ensuring that the other parts of the organization understand and agree to accept the services provided and provide the required information to the incident management function. If that does not happen, the IM function may not be able to perform effectively. Defining roles, responsibilities, and interfaces among groups of people performing incident management capabilities is needed to ensure everyone knows what their job is and how to work efficiently with other groups to detect, analyze, and respond to incidents.

The plans that are developed will establish and sustain the incident management function in terms of how it will function, communicate, and deal with incidents when they occur. The core processes are needed to define how the various key activities will be carried out, and the essential tools needed by the incident management function must be acquired. Chief among these tools is the incident repository where all the information relevant to incidents will be retained. This repository allows not only the immediate analysis of current incidents but also later analysis for trends and patterns, forensic analysis, and so forth.

Finally, no incident management function can be effective if it operates in isolation. IM personnel must establish trusted relationships with other experts to be aware of events and other types of attacks going on outside the organization and to reach back for additional expertise and help when faced with a new or unprecedented form of incident or the need for new tools. It takes time to get these relationships established and maintain them. This needs to be done as part of preparing.

Within the Prepare category, the subcategories and their capabilities include the following:

1.1 Establish IM Function—Establishing the IM function requires formal recognition and acceptance of its existence and its mission, who the people are who perform the activities and what they do, and defining how it works with other groups.

- 1.1.1 An incident management function or CSIRT has been officially designated by the organization head or chief information officer (CIO).
- 1.1.2 An incident management plan has been developed and implemented for the organization.
- 1.1.3 Roles and responsibilities are documented for key incident management activities throughout the organization and followed.
- 1.1.4 Formal interfaces for conducting organizational incident management activities are defined and maintained.
- 1.1.5 Trusted relationships are maintained with experts who can give technical and nontechnical advice and information.

1.2 Core Processes and Tools—An incident management function needs to establish the core practices and the basic tools that will be required for effective performance of incident management activities. That includes understanding how work will be managed, incident information will be retained, and how the potential for insider threat can be controlled.

- 1.2.1 A communication plan for incident management activities has been established and disseminated.
- 1.2.2 An IM information management plan is established and followed.
- 1.2.3 An inventory exists of mission-critical systems and data.
- 1.2.4 Workflow management processes and/or systems are implemented.
- 1.2.5 A central repository exists for recording and tracking security events and incidents.
- 1.2.6 Security events and incidents are categorized and prioritized according to organizational guidance.
- 1.2.7 An insider threat program exists within the organization.

1.1 ESTABLISH IM FUNCTION

1.1.1 An incident management function or CSIRT has been officially designated by the organization head or chief information officer (CIO).

Priority II

Clarification

The intent of this capability is to determine whether a group(s) or CSIRT has been established as the officially designated authority for incident management functions within the organization. This helps ensure the senior executives' support of the incident management mission, thereby helping the organization's members to understand the CSIRT's or incident management function's role and authority. Such a designation can be made through an official policy statement, an executive memo, or a simple announcement. Having only a procedure that lists the specific function is insufficient. Clearly designating the roles and responsibilities for incident management improves the reaction time and effort when managing incidents. If an incident management function is not specifically designated or appointed (either formally or informally), it will have difficulty operating consistently and effectively, or being recognized by the organization.

Team Guidance

The team should look for an organizational policy or other formal document that designates the CSIRT or other specific group such as the SOC as being responsible for incident management.

If a CSIRT or SOC has not been designated, the team should determine if another area of the organization has been given responsibility for the organization's incident management function. If that is the case, the alternative group should be assessed against this capability.

The team should look for evidence that all personnel within the organization are aware of the roles and levels of authority associated with incident management, as established by the organization's senior executive management.

References

Regulatory References: None

[indirect]

FISMA Sec 3544 *Federal agency responsibilities* (a)(4) [OLRC 2003]

> "(a) IN GENERAL—The head of each agency shall …:
> (4) ensure that the agency has trained personnel sufficient to assist the agency in complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines"

Guidance References:

NIST SP 800-53 Rev. 4 *Security and Privacy Controls for Federal Information Systems and Organizations* [NIST 2013]

> "IR-1 INCIDENT RESPONSE POLICY AND PROCEDURES
>
> **Control:** The organization:

(a.) Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:

1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and

(b.) Reviews and updates the current:

1. Incident response policy [Assignment: organization-defined frequency]; and
2. Incident response procedures [Assignment: organization-defined frequency].

IR-2 INCIDENT RESPONSE TRAINING

Control: The organization provides incident response training to information system users consistent with assigned roles and responsibilities:

(a.) Within [Assignment: organization-defined time period] of assuming an incident response role or responsibility;

(b.) When required by information system changes; and

(c.) [Assignment: organization-defined frequency] thereafter."

[indirect]

NIST SP 800-62 Rev 1 *Computer Security Incident Handling Guide* [Cichonski 2012]

"Sec 2.3.1 Policy Elements

…most policies include the same key elements: Statement of management commitment; Purpose and objectives of the policy; Scope of the policy (to whom and what it applies and under what circumstances);Definition of computer security incidents and related terms; Organizational structure and definition of roles, responsibilities, and levels of authority; should include the authority of the incident response team to confiscate or disconnect equipment and to monitor suspicious activity, the requirements for reporting certain types of incidents, the requirements and guidelines for external communications and information sharing (e.g., what can be shared with whom, when, and over what channels), and the handoff and escalation points in the incident management process; Prioritization or severity ratings of incidents; Performance measures (as discussed in Section 3.4.2); Reporting and contact forms."

Organization Response

Examples of Evidence Sought

- ❑ Organizational policy or other formal document designating the CSIRT, SOC, or other group as being responsible for the incident management function
- ❑ Written artifacts from the organization's executive management that informally designate the CSIRT, SOC, or other group/person as the principal incident handling POC
- ❑ Observation or demonstration of mechanisms for policy dissemination, archiving, and retrieval showing how they have been used for the official designation of incident management authority

Scoring Criteria	Yes	No	Evidence
Required			
1.1.1.01 Prerequisite: The constituency supported by the incident management function has been defined.	❒	❒	
1.1.1.02 Control: Executives in the organization provide visible support for the incident management mission and chain of command of the incident management function.	❒	❒	
1.1.1.03 Activity: A CSIRT, SOC, or other group has been established as the officially designated authority for incident management functions within the organization.	❒	❒	
1.1.1.04 Activity: An entity or specific person has been designated as the incident management "lead."	❒	❒	
Recommended Best Practices			
1.1.1.05 Activity: A policy or other official designation is documented and distributed throughout the organization or otherwise made available.	❒	❒	
Institutional and Quality Improvement			
1.1.1.06 Quality: Personnel know where the written organizational policy or formal declaration is located.	❒	❒	
1.1.1.07 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒
Not Applicable		❒	**Not Observed**	❒

Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement
• Document this designation in an official written publication, memo, or policy, and make it easily accessible to the organization. • Build mechanisms for educating the organization about the roles and responsibilities of incident management personnel. This task might include adding such information and the corresponding appointment order or announcement to orientation materials, incident reporting guidelines, employee handbooks, and other similar materials.

1.1 ESTABLISH IM FUNCTION

1.1.2 An incident management plan has been developed and implemented for the organization.

Priority I

Clarification

This capability focuses on ensuring that documented guidance exists that outlines activities, roles, and responsibilities for reporting, detecting, analyzing, responding to, and recovering from computer security (cyber) incidents. This is needed to ensure a consistent, quality-driven, and repeatable incident management process is in place that is known by and followed throughout the organization.

Having such a plan or documented guidance in place provides the organization with a standard operating procedure for handling incidents and vulnerabilities that may threaten or impact critical business operations and information. It also helps the organization be proactive by being able to engage the process immediately when an attack or other malicious activity is detected, rather than trying to figure out what steps need to be taken while already in the middle of an incident. By being prepared and knowing what steps to follow, which resources to call or that are available, and what policies and procedures to adhere to, the response can be performed in a faster manner resulting in quicker containment, eradication, and response activities, and lower the impact and damage to the organization.

An incident management plan should include at least the following components [6]:

- Defined purpose and structure of the incident management function
- Outlined workflow for handling incidents across the incident management function and other parts of the organization
- Description of the services performed by the incident management function
- Defined goal for the outcome of the response—i.e., collect evidence, coordinate information sharing, resolve incident
- Defined scope of the type of incidents handled and not handled
- Key people responsible for initiating and executing the plan
- Defined roles and responsibilities across the organization for reporting, detecting, analyzing, and responding to incidents
- Authority for performing various incident management/response activities
- Guidelines for determining who coordinates the incident
- High-level guidelines for what type of incidents to report and how to report them (This is documented in more depth in capabilities 4.1.1 and 4.1.2, which focus on incident reporting.)
- Guidelines for managing incidents throughout their lifecycle, including closing incidents and performing postmortems.
- Guidelines for who to notify and in what timeframe (could also be in the communication plan)

[6] Note that additional detailed plans and policies may exist for specific aspects. This is the higher level concept of operations for the whole incident management plan.

- Key data handling guidance and pointers to more detail in the information management plan outlined in capability 1.2.2
- Guidance for contacting and working with Human Resources (HR), Legal Counsel, Business Units, Management and other parts of the organization
- Guidance for contacting external stakeholders or collaborators
- Guidance for pulling in additional staff or surge support

Some incident management plans continue specific steps for handling specific types of incidents (i.e., playbooks). This can include incident scenarios and potential mitigations.

Team Guidance

The incident management plan can have many names: it may be documented as an incident response plan, as a Concept of Operations document (CONOPS), or even as a charter. If the document that has been created by the organization or incident management function contains the components listed in the clarification or in the indicators then it is acceptable and the capability is met.

Support can be provided on a 24x7 basis without having people in chairs. They can, for example, be on call with a requirement to respond within a specific time-frame. A defined process would address notifying IM staff and handling critical incidents outside business hours.

It is also possible that the incident management plan will be part of a larger risk management plan or continuity of operations (COOP) plan. Again, as long as the incident management components are called out, that is also acceptable.

It is also possible that the Communication Plan outlined in capability 1.2.1 may be contained as part of this incident management plan.

References

Regulatory References: None

Guidance References:

NIST 800-61 Rev. 2 *Computer Security Incident Handling Guide* [Cichonski 2012]

> "2.3.2 Plan Elements
>
> Organizations should have a formal, focused, and coordinated approach to responding to incidents, including an incident response plan that provides the roadmap for implementing the incident response capability. Each organization needs a plan that meets its unique requirements, which relates to the organization's mission, size, structure, and functions. The plan should lay out the necessary resources and management support. The incident response plan should include the following elements: Mission; Strategies and goals; Senior management approval; Organizational approach to incident response; How the incident response team will communicate with the rest of the organization and with other organizations; Metrics for measuring the incident response capability and its effectiveness; Roadmap for maturing the incident response capability; How the program fits into the overall organization."

NIST 800-53 Rev. 4 *Security and Privacy Controls for Federal Information Systems and Organizations* [NIST 2013]

> "IR-8 INCIDENT RESPONSE PLAN
>
> **Control:** The organization:

(a.) Develops an incident response plan that

1. Provides the organization with a roadmap for implementing its incident response capability;
2. Describes the structure and organization of the incident response capability;
3. Provides a high-level approach for how the incident response capability fits into the overall organization;
4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
5. Defines reportable incidents;
6. Provides metrics for measuring the incident response capability within the organization;
7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
8. Is reviewed and approved by [*Assignment: organization-defined personnel or roles*];

(b.) Distributes copies of the incident response plan to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements];

(c.) Reviews the incident response plan [*Assignment: organization-defined frequency*];

(d.) Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;

(e.) Communicates incident response plan changes to [*Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements*]; and

(f.) Protects the incident response plan from unauthorized disclosure and modification."

Organization Response

Examples of Evidence Sought

- ❑ A documented incident management plan
- ❑ A list of documented roles and responsibilities
- ❑ A list of stakeholder and constituent POCs who need to be notified
- ❑ A list of SMEs who can be called in for technical or surge support
- ❑ Artifacts related to the incident management plan such as forms and templates for reporting or tracking incidents
- ❑ Corresponding policies, procedures, and guidance that supports the incident management plan
- ❑ Organizational diagram showing the incident management function components
- ❑ Observation of incident management personnel following the plan during an incident

Scoring Criteria	Yes	No	Evidence
Required			
1.1.2.01 Control: Documented event/incident handling policies exist, including • provided services • any relevant criteria and limitations • clearly defined roles and responsibilities	❒	❒	
1.1.2.02 Control: Incident management support is provided on a 24x7 basis.	❒	❒	
1.1.2.03 Control: Organizational personnel are provided with documentation that outlines incident handling services (e.g., in a service level agreement [SLA], MOU, email, webpage announcement).	❒	❒	
1.1.2.04 Control: A list of POCs for coordination, notification, and technical support exists.	❒	❒	
1.1.2.05 Activity: An incident management plan is documented and implemented.	❒	❒	
1.1.2.06 Activity: Incidents are handled according to the incident management plan.	❒	❒	
Recommended Best Practices			
1.1.2.07 Control: Documented policy exists requiring 24/7 support.	❒	❒	
1.1.2.08 Control: Defined guidance and scenarios for responding to particular types of incidents exists (for example distributed denial of service [DDoS], personally identifiable information [PII] spillage, malware installation, persistent threats, etc.).	❒	❒	
Institutional and Quality Improvement			
1.1.2.09 Control: Documented procedures exist for event/incident handling, including • guidelines for 24/7 support • methods for responding to various incident types • escalation criteria	❒	❒	

• special instructions for critical system response-time goals based on at least the category/severity of the threat/incident			
1.1.2.10 Quality: Personnel are aware of, knowledgeable of, and consistently follow the procedures, processes, methodologies, and technologies for collecting and using this information.	❒	❒	
1.1.2.11 Quality: A process and criteria exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒	
Not Applicable		❒	**Not Observed**	❒	

Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement
None

1.1 ESTABLISH IM FUNCTION

1.1.3 Roles and responsibilities are documented for key incident management activities throughout the organization and followed.

Priority I

Clarification

The intent of this capability is to ensure that roles and responsibilities are clearly assigned to incident management personnel and are understood. Without clear role assignments and corresponding responsibilities delineated, staff often do not understand the scope of their job function and are not able to perform it effectively. Defined roles and responsibilities make it clear that all services are covered and that all staff know what they should be doing on a daily basis. Roles and responsibilities can also be used to determine competency requirements and knowledge, skills, and abilities (KSAs) needed to perform assigned functions. These competencies and KSAs can be built into a training or development plan. Roles and responsibilities can be documented via an organizational chart, a POC list, or some other written document.

Team Guidance

This capability has a strong tie to the 1.1.4 formal interface capability. If interfaces are poorly defined, this capability will be difficult to meet, since roles and responsibilities across the organization may not be adequately defined, clarified, or communicated. This function might not be applicable in small organizations, where only a few staff members are involved in incident management and interchangeably share the associated roles and responsibilities. If those roles and responsibilities are spread out to multiple parts of the organization, the team will need to verify the documentation and implementation of as many of them as possible.

References

Regulatory References: None

Guidance References:

NIST SP 800-61 Rev 2 *Computer Security Incident Handling Guide* [Cichonski 2012]

> "Sec 2.4.4 Dependencies Within Organizations
> It is important to identify other groups within the organization that may be needed to participate in incident handling so that their cooperation can be solicited before it is needed. Every incident response team relies on the expertise, judgment, and abilities of others, including— […] Management […] Information Assurance […]IT Support […] Legal Department […] Public Affairs and Media Relations […] Human Resources […] Business Continuity Planning […] Physical Security and Facilities Management […]"

Organization Response

Examples of Evidence Sought
❑ Organizational chart ❑ Documentation of incident management roles and responsibilities ❑ Mechanisms for documenting and disseminating roles and responsibilities

Scoring Criteria	Yes	No	Evidence
Required			
1.1.3.01 Control: An organizational chart exists showing the structure and activities of the incident management function.	❒	❒	
1.1.3.02 Activity: The roles and responsibilities are defined.	❒	❒	
1.1.3.03 Activity: The work and information flow for incident management activities (e.g., work process flows, flowcharts, or procedures) are documented, including the nature of information exchanged and any requirements associated with the interfaces between different groups.	❒	❒	
1.1.3.04 Activity: Documented roles and responsibilities are reviewed at least yearly to ensure accurate reflection of who performs IM activities.	❒	❒	
Recommended Best Practices			
1.1.3.05 Control: A code of conduct for incident management personnel is established and followed.	❒	❒	
1.1.3.06 Activity: If constituents are responsible for some or all of the incident response activities, roles and responsibilities are defined (e.g., SLAs, MOUs, email).	❒	❒	
Institutional and Quality Improvement			
1.1.3.07 Quality: The organizational chart is up to date.	❒	❒	
1.1.3.08 Quality: The organizational chart (or other appropriate document) includes descriptions of the roles and responsibilities of all key positions.	❒	❒	

1.1.3.09 Quality: Personnel are familiar with their roles and responsibilities, and the organization's internal reporting structure.	❒	❒	
1.1.3.10 Quality: The assigned roles and responsibilities are reviewed at least annually for effectiveness and efficiency, and improvements are made as needed.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒
Not Applicable		❒	**Not Observed**	❒

Evidence Collected

Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement

- Develop an up-to-date organizational chart, written charter, or workflow that identifies all parties involved in incident management and their assigned roles and responsibilities. This information should be reviewed and updated periodically to include any changes in personnel and responsibilities.
- Make any document that describes incident management roles and responsibilities easily accessible in both hard-copy and electronic form. Information about incident management roles and responsibilities should also be included in training materials, orientation packets, and handbooks for those involved in incident management activities (including applicable organization employees).

1.1 ESTABLISH IM FUNCTION

1.1.4 Formal interfaces for conducting incident management activities are defined and maintained.

Priority I

Clarification

The intent of this capability is to ensure that interfaces among the groups involved in incident management functions are described and understood by all participants. This capability focuses on the interfaces between the various groups involved in incident management functions, including internal components (e.g., a CSIRT, ISO, patch management group, firewall group, or network administration group) and external groups (e.g., law enforcement [LE], internet service providers [ISPs], incident response contractors or subcontractors, or other security groups like CERT/CC).

Team Guidance

The team might need to assess multiple interfaces when assessing this capability. The number of interfaces assessed will depend on the number of groups that perform incident management activities. The simplest means of assessing this capability is to gather information about the various interfaces and then provide a summary answer for how well interfaces, in general, are handled. If the team decides it is necessary, it can assess each interface separately and then document an individual score for each. This decision should be based on the organization's needs and the scope that has been agreed to. For example, if the organization wants to address a particular problem area, it may be beneficial to do that as a separate score.

During an assessment, it might be difficult to interview external groups that interface with an organization. It may be practical to assess only organization personnel about their perspectives on a given interface. All interfaces—both formal and informal—should be identified and discussed. The best practice for this capability is for interfaces to be formalized. However, in many cases, interfaces among groups will be informal and undocumented. If there are external parties involved, make sure they are defined.

As an assessment is being performed, the assessment team might identify additional groups that need to be interviewed (i.e., groups that are not currently scheduled to participate in the assessment). Assessment teams should be careful not to extend the assessment unnecessarily to include peripheral groups whose participation in incident management is marginal.

This capability should be scored as "Not Applicable" if there is no interface or *need* for one between groups within the organization. While an interface may not currently exist, the need for one might be raised during the course of the assessment. If such a need is discussed during the assessment, the assessment team can use this capability to show the organization that the interface should be included in an improvement plan and that all participating groups should be involved in refining it.

Assessment team members should note the following items when assessing this capability:

- The ways in which an interface is documented can vary greatly—from a series of email exchanges between managers to formal contracts. As long as the required aspects of the interface are documented and the personnel responsible for the interface know about and meet the requirements, the organization can decide how formal to make the documentation.

- The team should be able to determine from discussions with personnel whether those personnel know how to appropriately work with other groups (e.g., by assessing how well people can describe an interface). More importantly, personnel should be able to demonstrate how they perform their tasks and activities (e.g., show the forms they must complete, describe the process for providing and receiving inputs and outputs to and from the interface).

References

Regulatory References: None

Guidance References: None

Organization Response

Examples of Evidence Sought

- ❑ Documentation of the interface (e.g., email, MOU, memorandum of agreement [MOA], letter of agreement [LOA], SLA, procedure, formal contract, work process flows, organizational charts)
- ❑ Samples of information or data exchanged between groups
- ❑ Up-to-date contact information (e.g., phone, email, Pretty Good Privacy [PGP] keys, certificates)
- ❑ Alternate forms of communication for POCs (and alternates) for both parties

Scoring Criteria	Yes	No	Evidence
Required			
1.1.4.01 Control: Personnel in both groups are appropriately trained on the requirements and relevant technology for implementing this interface.	❒	❒	
1.1.4.02 Control: The interface is documented for both parties (e.g., guidance, email, MOU, MOA, LOA, SLA, procedure, formal contract) including roles and responsibilities, information exchange requirements (e.g., timeframes, criteria), verification of information receipt, and the decision-making process.	❒	❒	
1.1.4.03 Activity: Defined interfaces are established with internal and external parties performing incident management activities.	❒	❒	

1.1.4.04 Activity: Both parties follow the defined interface guidance when performing their work.	❒	❒	
Recommended Best Practices			
1.1.4.05 Control: The interface documentation includes the process and POCs used to resolve conflicts or issues.	❒	❒	
1.1.4.06 Control: The interface documentation includes the process for reviewing and modifying the interface agreement.	❒	❒	
1.1.4.07 Activity: Mock exercises are held to test the effectiveness of the interface under different conditions (e.g., normal, duress).	❒	❒	
Institutional and Quality Improvement			
1.1.4.08 Quality: Personnel are aware of, knowledgeable of, and consistently use the procedures, processes, methodologies, and technologies for performing this activity.	❒	❒	
1.1.4.09 Quality: A process and criteria exist for evaluating and improving the quality of the interfaces associated with this activity.	❒	❒	
1.1.4.10 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**		❒
Not Applicable		❒	**Not Observed**		❒
Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes
Suggestions for Improvement
None

1.1 ESTABLISH IM FUNCTION

1.1.5 Trusted relationships are maintained with experts who can give technical and nontechnical advice and information.

Priority III

Clarification

The intent of this capability is to show that incident management personnel have contacts with internal and external experts, trust them, and keep their contact information current to ensure rapid coordination when their assistance is required. Experts could include the CERT Coordination Center [CERT/CC], the Forum of Incident Response and Security Teams [FIRST], or vendors.

Incident management staff will be better positioned to quickly respond to situations that arise if they can

- securely and effectively coordinate, collaborate, and exchange information with internal and external experts on a regular basis without error or misunderstanding
- call upon knowledgeable and trusted specialists for added expertise

The internal experts or contacts can provide assistance with technical aspects of incident management such as information technology (IT) or application experts as well as nontechnical aspects, such as public relations, legal, and HR issues. Incident management personnel without trusted contacts are isolated and may be in trouble in times of need.

The external experts may include other security experts, CSIRTs, vendors, LE, and others external to the organization who can be called on when needed (for incident coordination, situational awareness, incident analysis, product support for vendor applications, anti-virus software [AVS], and vulnerabilities, etc.). Incident management personnel must be able to securely and effectively coordinate, communicate, and exchange information with external experts on a regular basis without error or misunderstanding.

There is no time during fast-moving incidents to try and work through approved channels to locate experts, have questions reviewed and approved, and wait for answers. These trusted relationships must be established ahead of time and be easily leveraged to assist with analysis, correlation, guidance, and gathering other useful information that the IM function needs. Trust takes time and effort to build and keep.

Team Guidance

Depending on the nature of "trust" within the organization and with external contacts, none of the listed evidence may be available to assess, or different items might be reviewed.

If evidence is available, the team should look for an updated list of experts and a process used to ensure that this list of experts is maintained and accurate, and that the experts are properly vetted.

References

Regulatory References: None

[indirect]
FISMA Sec 3544 *Federal agency responsibilities* (b)(7)(B) [OLRC 2003]

"(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] that includes— […]
(7) procedures for detecting, reporting, and responding to security incidents […] including— […]
(B) notifying and consulting with the Federal information security incident center referred to in section 3546 [US-CERT]"

Guidance References:

NIST SP 800-61 Rev 2 *Computer Security Incident Handling Guide* [Cichonski 2012]

"Sec 2.3.4 Sharing Information With Outside Parties
[p 8-13]

Organizations often need to communicate with outside parties regarding an incident, and they should do so whenever appropriate, such as contacting LE, fielding media inquiries, and seeking external expertise. […]

The following sections provide guidelines on communicating with several types of outside parties […]

2.3.4.1 The Media
[…]

2.3.4.2 Law Enforcement
[…]

2.3.4.3 Incident Reporting Organizations
FISMA requires Federal agencies to report incidents to the United States Computer Emergency Readiness Team (US-CERT),[7] which is a government wide incident response organization that assists Federal civilian agencies in their incident handling efforts.

Each agency must designate a primary and secondary POC with US-CERT and report all incidents consistent with the agency's incident response policy.

All organizations are encouraged to report incidents to their appropriate CSIRTs. If an organization does not have its own CSIRT to contact, it can report incidents to other organizations, including Information Sharing and Analysis Centers (ISACs). […]

2.3.4.4 Other Outside Parties
[p 12-13] "An organization may want to discuss incidents with several other groups, including those listed below. […]

- Organization's ISP […]
- Owners of Attacking Addresses […]
- Software Vendors […]
- Other Incident Response Teams […]
- Affected External Parties […]"

NIST 800-53 Rev. 4 Security and Privacy Controls Federal Information Systems and Organizations [NIST 2013]

- SA-9 (3)

EXTERNAL INFORMATION SYSTEMS | ESTABLISH / MAINTAIN TRUST RELATIONSHIP WITH PROVIDERS

[7] http://www.us-cert.gov/

The organization establishes, documents, and maintains trust relationships with external service providers based on [*Assignment: organization-defined security requirements, properties, factors, or conditions defining acceptable trust relationships*].

Supplemental Guidance: The degree of confidence that the risk from using external services is at an acceptable level depends on the trust that organizations place in the external providers, individually or in combination. Trust relationships can help organization to gain increased levels of confidence that participating service providers are providing adequate protection for the services rendered…"

Organization Response

Examples of Evidence Sought

- ❑ Up-to-date POC list for trusted experts with phone numbers, email addresses, and other contact information
- ❑ MOU/MOA/SLA or other documentation with the organization and the experts that defines the nature of the relationship and responsibilities
- ❑ Minutes, records, actions, and so forth of joint meetings, working groups, conferences, meetings, and technical exchanges
- ❑ Observation of personnel establishing or working with trusted expert (e.g., exchanging PGP/GNU Privacy Guard [GnuPG] keys with expert, vetting a new expert)

Scoring Criteria	Yes	No	Evidence
Required			
1.1.5.01 Control: A process exists for contacting and working with organizational experts.	❒	❒	
1.1.5.02 Control: Personnel are aware and knowledgeable of the relationships, documented POC list, and when and how to contact the POCs.	❒	❒	
1.1.5.03 Activity: Personnel establish and maintain the expert relationships documented in a POC list.	❒	❒	
1.1.5.04 Activity: Personnel contact and work with expert POCs as needed.	❒	❒	
Recommended Best Practices			
1.1.5.05 Control: MOU/MOA/SLA/NDA[8] or some other documentation between the organization and the external experts establishes the rules of engagement.	❒	❒	

[8] NDA stands for non-disclosure agreement.

1.1.5.06 Control: A documented policy or guidance exists for authorizing work with external groups and experts.	❒	❒	
1.1.5.07 Control: Documented procedures exist for vetting and approving new experts, establishing trust, and working with the experts.	❒	❒	
1.1.5.08 Activity: Interactions with internal experts should be approved by the experts' managers.	❒	❒	
1.1.5.09 Activity: Relationships with experts are established in advance of incident occurrence.	❒	❒	
Institutional and Quality Improvement			
1.1.5.10 Quality: Personnel are aware of, knowledgeable of, and consistently follow the procedures for this activity.	❒	❒	
1.1.5.11 Quality: A process and criteria exist for evaluating how well interfaces are managed and the quality of exchanged information and services.	❒	❒	
1.1.5.12 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒	
Not Applicable		❒	**Not Observed**	❒	
Evidence Collected					
Document Review		Interviews		Direct Observation	
Notes					

Suggestions for Improvement
• Develop a matrix of the needed skills and knowledge, the people who have those skills and knowledge, and their contact information.

1.2 CORE PROCESSES AND TOOLS

1.2.1 A communication plan for incident management activities has been established and disseminated.

Priority II

Clarification

This capability focuses on the organization having an established and institutionalized communication plan for its incident management activities. During an incident it is critical that the right people receive the right information in the right timeframe. This is important from both a management notification standpoint and an incident response and coordination standpoint. Management often needs to be notified of an incident that is reported for reasons beyond impact to the organization. Sometimes they need to know that a report was received from a critical stakeholder to ensure that they are aware of the situation in case they are asked about it; this type of notification is more for internal awareness. From an incident response and coordination standpoint, a communication plan may outline what type of alerts or warnings are to be sent to the organization, along with what type of response steps are being recommended to constituents. The communication plan may also include guidance on whether or not the incident has to be reported up a particular chain of management or to another coordination point such as CERT/CC, an investigative unit, or LE in the case of a crime.

The communication plan should be known and established ahead of time. Information within the plan should include at a minimum

- the individuals, groups, and designated POCs to be contacted
- thresholds for whether to contact someone
- the process and mechanism for contacting, including needed secure mechanisms
- the timeframe for contacting
- a description of what the individual is to do with the communicated information (This is particularly focused on response. For example, is the information communicated to be acted on by the recipient as part of the incident response, or is it a simple FYI notification?)

This communication plan may be part of a larger organizational plan or crisis management plan. It should align with the organizational mission and supporting policies, and include guidance for when and how to contact, notify, and coordinate with LE, HR, IT, other organizational security groups, and any external stakeholders.

Team Guidance

The team should look for evidence that the communication plan exists and is known throughout the incident management function and that personnel follow it. The plan should also be periodically updated and should be covered in any training for new staff. The team should also look for evidence that the plan has been disseminated to organizational personnel.

If there is ONLY a general communication plan for the organization and not a separate one for incident management activities, ensure that there is a section within it that specifies what type of communications should occur regarding incident reporting, detection, or response. If there is nothing specific about incident management in the general plan, then this capability is NOT met.

A communication plan is not the same as an escalation plan. If only an escalation plan or chain of command document exits and no communication plan exists, then the capability is NOT met.

References

Regulatory References: None

Guidance References:

NIST 800-61 Rev. 2 *Computer Security Incident Handling Guide* [Cichonski 2012]

> "2.3.2 Plan Elements
>
> Organizations should have a formal, focused, and coordinated approach to responding to incidents, including an incident response plan that provides the roadmap for implementing the incident response capability….incident response plan should include the following elements:…How the incident response team will communicate with the rest of the organization and with other organizations
>
> 2.3.4 Sharing Information with Outside Parties
>
> Organizations often need to communicate with outside parties regarding an incident, and they should do so whenever appropriate, such as contacting LE, fielding media inquiries, and seeking external expertise. Another example is discussing incidents with other involved parties, such as Internet service providers (ISPs), the vendor of vulnerable software, or other incident response teams. Organizations may also proactively share relevant incident indicator information with peers to improve detection and analysis of incidents. The incident response team should discuss information sharing with the organization's public affairs office, legal department, and management before an incident occurs to establish policies and procedures regarding information sharing. Otherwise, sensitive information regarding incidents may be provided to unauthorized parties, potentially leading to additional disruption and financial loss. The team should document all contacts and communications with outside parties for liability and evidentiary purposes."

Organization Response

Examples of Evidence Sought

- ❑ Documented communication plan
- ❑ Memo or other evidence announcing and describing the communication plan that has been sent to the appropriate organizational personnel
- ❑ Training materials that describe the communication plan
- ❑ Sample materials sent according to the communication plan instructions and guidance
- ❑ Policies and procedures referencing the communication plans
- ❑ Demonstration of how information is disseminated according to communication plan
- ❑ Observation of information dissemination following the communication plan during a real incident
- ❑ Demonstration or observation of secure communications mechanisms
- ❑ Documented guidance for handling information commensurate with its sensitivity level

Scoring Criteria	Yes	No	Evidence
Required			
1.2.1.01 Control: A communication plan for incident management activities has been documented.	❒	❒	
1.2.1.02 Control: Guidance exists that specifies how communication is executed.	❒	❒	
1.2.1.03 Control: Personnel are appropriately trained in the processes and supporting technologies used to execute the plan.	❒	❒	
1.2.1.04 Control: A list of POCs and timeframes for when and who should be contacted is included in the communication plan.	❒	❒	
1.2.1.05 Control: Thresholds or triggers for whether constituents and external personnel and groups should be contacted have been established.	❒	❒	
1.2.1.06 Control: Incident management personnel are trained on how to communicate according to the communication plan.	❒	❒	
1.2.1.07 Activity: Designated organizational tools and mechanisms are used to communicate with appropriate personnel regarding incident management activities, including identified secure communications mechanisms.	❒	❒	
1.2.1.08 Activity: The communication plan is followed to notify and/or involve appropriate personnel about current incident activity and resolution.	❒	❒	
1.2.1.09 Activity: Guidelines for handling sensitive or confidential communication are followed when handling such data or information.	❒	❒	
Recommended Best Practices			
1.2.1.10 Control: The incident management communication plan aligns with the overall organizational communication plan.	❒	❒	
1.2.1.11 Control: A list of document types that will be used to communicate with stakeholders is established and shared with appropriate internal and external personnel.	❒	❒	

1.2.1.12 Quality: A process exists to keep all POC lists and source information up to date.	❒	❒	
Institutional and Quality Improvement			
1.2.1.13 Quality: The communication plan is formally tested on at least a yearly basis.	❒	❒	
1.2.1.14 Quality: Personnel are aware of, knowledgeable of, and consistently follow the procedures, processes, methodologies, and technologies for collecting and using this information.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒	
Not Applicable		❒	**Not Observed**	❒	
Evidence Collected					
Document Review		Interviews		Direct Observation	
Notes					
Suggestions for Improvement					
None					

1.2 CORE PROCESSES AND TOOLS

1.2.2 An IM information management plan is established and followed. **Priority II**

Clarification

This capability focuses on having the right policies, guidance, and tools in place to appropriately handle, store, and disseminate incident and vulnerability data. Incident management functions, teams, or CSIRTs live and die by their ability to protect information, keep confidences, and build trust from their stakeholders and constituents. To do so, any data received must be handled commensurate with its sensitivity or security requirements and only relayed to authorized personnel including internal or external partners. An IM information management plan provides the guidance to do this and includes several policies, such as media relations, information disclosure, information classification schema, data retention, and acceptable use.

Handling incidents is always related to handling information. Information is always the key, regardless of whether specific information relates to a contact, a site, a product, a new vulnerability, an ongoing attack, or a password. Incident management functions receive a variety of information with multiple levels of sensitivity. Because much of the IM function's work revolves around constituent incidents and vulnerabilities, the data received, processed, and stored can include existing weaknesses and problem areas within the organization. Therefore, incident management data and information is a target for attacks including social engineering or exfiltration. Every piece of information received or created must be stored and protected for the entire time it is held by the incident management function. Tagging the information according to its type and sensitivity will facilitate continued appropriate handling.

Incident management functions must have a documented policy or guidance on information categorization (e.g., classification scheme for sensitivity). Without one, personnel will apply their own perceived categorization to each piece of information, or not attempt to differentiate it at all. As individual perceptions may differ, resulting in inconsistent and possibly inappropriate actions, a policy must be available to guide categorization.

It is important to define an information disclosure policy for the realm of incident response and beyond. One of the most important issues that an incident management function or team needs to pay attention to is how it is respected and trusted by its constituency and other teams. Without that trust and respect, a team will not be able to function successfully and effectively because people will be reluctant to report information to it. Without such a policy or guidance, personnel will not have consistent instructions on what they can say to whom and when as they handle calls and respond to email. Disclosure extends to dealing with the media. Most organizations also have a media relations policy detailing who is authorized to speak to the media and how requests from the media should be forwarded.

As part of garnering trust in the community and within the constituency, incident management personnel must be seen as always using their access to information in the proper way. This means only using equipment, software, and tools in an acceptable manner as outlined in an acceptable use policy or guidance.

Team Guidance

It is possible that there is an information management plan in place for the whole organization. If that is the case, the team should review it and look for the sections that specifically deal with

incident and vulnerability data. If that is not covered in the plan and there is no separate information management plan for incident management, then this capability is not met.

The plan can take many forms: it may be a policy or a set of guidance. The team should use the word "plan" in the broadest sense.

The media, information disclosure, and acceptable use documentation might not be a "policy" per se, but may be guidance or procedures. In that case, those are acceptable and meet the indicator.

The information classification schema is most likely (and should be) an organizational policy to ensure consistent use throughout the enterprise. The team should look for this broader policy and if there is a separate one for incident management, it should align with the organizational one. Information classification schema deals with identifying the sensitivity of data. For example, in the U.S. Federal government there are a series of labels and markings for classification levels as follows:

- Top Secret (TS)
- Secret
- Confidential
- Restricted
- Unclassified

References

Regulatory References:

Executive Order 12958 Classified National Security Information April 17, 1995

> "This order prescribes a uniform system for classifying, safeguarding, and declassifying national security information. "

[indirect]

FISMA Sec 3544 *Federal agency responsibilities* (a)2(B) [OLRC 2003]

> "(a) IN GENERAL. —The head of each agency shall —
>
> (2) ensure that senior agency officials provide information security for the information and information systems that support the operations and assets under their control, including through —
>
> (B) determining the levels of information security appropriate to protect such information and information systems in accordance with standards promulgated under section 11331 of title 40, for information security classifications and related requirements;"

Guidance References:

SP 800-53 Rev 4 *Security and Privacy Controls for Federal Information Systems and Organizations* [NIST 2013]

> "MP-3 MEDIA MARKING
>
> Control: The organization:
>
> (a.) Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information
>
> Supplemental Guidance: The term *security marking* refers to the application/use of human-readable security attributes. The term *security labeling* refers to the application/use of security attributes with regard to internal data structures within information systems (see AC-16). Information system media includes both digital and non-digital media. Digital media includes, for

example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Security marking is generally not required for media containing information determined by organizations to be in the public domain or to be publicly releasable. However, some organizations may require markings for public information indicating that the information is publicly releasable. Marking of information system media reflects applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. […]"

Organization Response

Examples of Evidence Sought

- ❑ Documented IM information management plan or policy
- ❑ Documented IM information classification schema
- ❑ Examples of IM information marked with the appropriate classification labels
- ❑ An information disclosure policy or guidance
- ❑ A media relations policy or guidance
- ❑ An acceptable use policy or guidance
- ❑ Demonstration of personnel handling incident and vulnerability data according to the IM information plan and related polices or guidance
- ❑ Case studies describing situations where the policies and guidance were followed when handling incident or vulnerability data

Scoring Criteria	Yes	No	Evidence
Required			
1.2.2.01 Control: An IM information management plan and related policies and processes are in place that detail how incident and vulnerability data and corresponding artifacts are handled, protected, and shared.	❒	❒	
1.2.2.02 Control: An organizational information classification schema is in place that identifies different levels of information sensitivity and outlines a process for handling and labeling data commensurate with its classification.	❒	❒	
1.2.2.03 Control: A media relations policy or guidance is established that describes how questions, calls, and other interactions from the media are handled related to incidents and vulnerabilities.	❒	❒	
1.2.2.04 Control: An information disclosure policy or guidance is implemented that describes what information can be distributed to whom and in what timeframe.	❒	❒	

1.2.2.05 Control: An acceptable use policy or guidance is implemented and followed that describes how incident management personnel can use organizational and incident management equipment and software.	❒	❒	
1.2.2.06 Control: A policy or guidance for data retention for incident and vulnerability information is defined and documented.	❒	❒	
1.2.2.07 Activity: Incident management personnel protect incident and vulnerability data and artifacts according to established policies and procedures.	❒	❒	
1.2.2.08 Activity: Incident management personnel disclose incident and vulnerability data and artifacts only to authorized people through authorized means.	❒	❒	
1.2.2.09 Activity: Incident management personnel handle incident and vulnerability data and artifacts commensurate with their level of sensitivity or classification.	❒	❒	
1.2.2.10 Activity: Incident management personnel retain data on incidents and vulnerabilities according to policy or guidance.	❒	❒	
Recommended Best Practices			
1.2.2.11 Control: New IM personnel orientation emphasizes the information management plan and corresponding policies and guidelines.	❒	❒	
Institutional and Quality Improvement			
1.2.2.12 Quality: The IM information management plan, media relations policy, information disclosure policy, information classification schema, data retention plan, and acceptable use policy are reviewed at least once a year to identify and implement updates.	❒	❒	
1.2.2.13 Quality: Personnel are aware of, knowledgeable of, and consistently follow the procedures, processes, methodologies, and technologies for collecting and using this information.	❒	❒	
1.2.2.14 Quality: A process and criteria exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	

1.2.2.15 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.			❒	❒	
Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒	
Not Applicable		❒	**Not Observed**	❒	
Evidence Collected					
Document Review		Interviews		Direct Observation	
Notes					
Suggestions for Improvement					
None					

1.2 CORE PROCESSES AND TOOLS

1.2.3 An inventory exists of mission-critical systems and data. **Priority I**

Clarification

This capability ensures that constituent mission-critical systems and data have been identified within the organization and an up-to-date inventory has been provided to incident management personnel so a better prioritized response and remediation can be performed. This capability is an essential part of the Protect, Detect, Respond, and Sustain categories.

This capability focuses on understanding the constituents' critical systems and the data that must be protected. Current information should be available about what is on constituents' networks and systems to best assess protection requirements and ensure a timely and appropriate response. Having up-to-date information also helps ensure legal compliance with regulations or laws (e.g., to make sure information is released or accessed in an authorized fashion). When an event, incident, or vulnerability is reported, this information allows impacts to be assessed in light of the data's or system's criticality. If the location of critical data is not known, notification of end users and other relevant parties as stipulated by compliance laws may be delayed or not occur at all.

Team Guidance

If an inventory of mission-critical systems and data, exists but incident management personnel cannot access it, this capability is not met.

If possible, up to date configuration information should be available for all supported organizational networks and systems. Configuration information can include

- a list of internet protocol (IP) address ranges and responsible administrative personnel or ISOs
- the latest organizational network diagrams
- an up-to-date inventory of constituent information systems, network components, application software, operating systems (OSs), and network services used by the organization
- a list of network access points and their operational importance

References

Regulatory References: None

[indirect]

Federal Information Processing Standards (FIPS) 199 *Standards for Security Categorization of Federal Information and Information Systems* [NIST 2004]

> "FIPS Publication 199 addresses the first task cited—to develop standards for categorizing information and information systems. Security categorization standards for information and information systems provide a common framework and understanding for expressing security that, for the Federal government, promotes: (i) effective management and oversight of information security programs, including the coordination of information security efforts throughout the civilian, national security, emergency preparedness, homeland security, and

law enforcement communities; and (ii) consistent reporting to the Office of Management and Budget (OMB) and Congress on the adequacy and effectiveness of information security policies, procedures, and practices."

Guidance References:

NIST 800-61 Rev 2 *Computer Security Incident Handling Guide* [Cichonski 2012]

"Sec 3.2.6 Incident Prioritization
Prioritizing the handling of the incident is perhaps the most critical decision point in the incident handling process. Incidents should not be handled on a first-come, first-served basis as a result of resource limitations. Instead, handling should be prioritized based on the relevant factors, such as the following:

Functional Impact of the Incident. Incidents targeting IT systems typically impact the business functionality that those systems provide, resulting in some type of negative impact to the users of those systems. Incident handlers should consider how the incident will impact the existing functionality of the affected systems. Incident handlers should consider not only the current functional impact of the incident, but also the likely future functional impact of the incident if it is not immediately contained."

CSIRT Case Classification[9] [Reid 2004]

"It is critical that the CSIRT provide consistent and timely response to the customer, and that sensitive information is handled appropriately. This document provides the guidelines needed for CSIRT Incident Managers (IM) to classify the case category, criticality level, and sensitivity level for each CSIRT case. This information will be entered into the Incident Tracking System (ITS) when a case is created. Consistent case classification is required for the CSIRT to provide accurate reporting to management on a regular basis. In addition, the classifications will provide CSIRT IM's with proper case handling procedures and will form the basis of SLAs between the CSIRT and other Company departments.

III Criticality Classification

Typically the IM will determine the criticality level. In some cases it will be appropriate for the IM to work with the customer to determine the criticality level…

IV Sensitivity Classification

The sensitivity matrix below helps to define "need to know" by classifying cases according to sensitivity level. Typically the IM will determine the sensitivity level. In some cases it will be appropriate for the IM to work with the customer to determine the sensitivity level."

NIST SP 800-53 Rev. 4 Security and Privacy Controls for Federal Information Systems and Organizations [NIST 2013]

"CM-8 Information System Component Inventory"

Organization Response

Examples of Evidence Sought

- ❑ Up-to-date list or database of constituents' critical systems and data
- ❑ Up-to-date list of POCs for constituents' critical systems and data

[9] http://www.first.org/_assets/resources/guides/csirt_case_classification.html

Scoring Criteria	Yes	No	Evidence
Required			
1.2.3.01 Prerequisite: Criteria exist that define which systems and data are mission critical.	❒	❒	
1.2.3.02 Control: A documented process exists establishing an inventory of critical systems and data.	❒	❒	
1.2.3.03 Control: A documented process exists for contacting the personnel responsible for critical systems and data.	❒	❒	
1.2.3.04 Control: Incident management personnel are trained appropriately on the policies and technologies employed to obtain, store, and use this inventory.	❒	❒	
1.2.3.05 Activity: An inventory of mission-critical systems and data, and associated POCs is established and maintained.	❒	❒	
1.2.3.06 Activity: Incident management personnel have access to an up to date and accurate list of mission-critical systems and data.	❒	❒	
Recommended Best Practices			
1.2.3.07 Activity: A database or other mechanism is used to track mission-critical systems and data, and corresponding POCs.	❒	❒	
1.2.3.08 Activity: The critical inventory is archived in a secure and protected manner.			
1.2.3.09 Quality: Fields in constituents' incident handling and tracking system capture the mission criticality of affected or compromised systems and data.	❒	❒	
Institutional and Quality Improvement			
1.2.3.10 Control: Documented procedures exist that describe the process and method by which the inventory of mission-critical systems and data is obtained, stored, and used.	❒	❒	
1.2.3.11 Quality: The inventory is sufficiently detailed to enable analysts to determine whether an event or incident affects mission-critical systems and data.	❒	❒	

1.2.3.12 Quality: Personnel are aware of, knowledgeable of, and consistently follow the procedures, processes, methodologies, and technologies for collecting and using this inventory.	❒	❒	
1.2.3.13 Quality: A process and criteria exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	
1.2.3.14 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒
Not Applicable		❒	**Not Observed**	❒

Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement

- When incident management personnel (especially those in distributed control environments) don't have direct access to configuration information for each identified critical system or asset, a formal interface should be established with the part of the organization that does. This interface can also be used as a means of coordinating improvements to system and network configurations based on trend analysis, incident history, and incident management staff expertise.
- Where possible, incident management personnel should be involved in the constituent change management process to ensure that knowledge about infrastructure changes is appropriately shared from a security perspective and to allow incident management personnel to have security-related input in needed changes.

1.2 CORE PROCESSES AND TOOLS

1.2.4 Workflow management processes and/or systems are implemented.

Priority III

Clarification

Incident handling continuity problems arise as teams have to deal with many problems, large amounts of data, multiple sources of data, and changing events over long periods of time.

This capability focuses on the need to have processes and mechanisms in place to ensure incident management personnel can get to information when needed, including during hand-offs of ongoing incidents. This also requires that all information about an incident and its related artifacts is captured throughout the incident handling lifecycle. In addition to the initial documentation of the incident on an incident reporting form, this information includes documentation of additional information gathered during analysis and response. Analysis documentation should include what type of analysis was done, how it was done (so it can be repeated if necessary), and the conclusions reached. Response actions to be documented include preliminary response actions, first responder actions, or actions taken to preserve and protect incident artifacts, evidence, or chain of custody. It can also include courses of action taken, recovery actions taken, and any follow-ups done with victim sites or collaborators. Continuous and frequent updates of the incident information provide a more complete understanding of the incident. This type of updating also provides a platform to broadly characterize adversarial activity and enables the team to combat this activity tactically and strategically.

Incident management functions or teams can receive information in multiple ways: incident reports, email, system log files, phone, hard-copy files, web forms, network sensors, and social media. Correlating this information and tagging and storing related information is not easy. Methods must be in place to allow for capturing and collating all these types of information. Making this information available to everyone at any time is even more difficult.

Workflow management—managing the flow of events that are part of the incident management function's daily activity—is essential to ensure continuity of IM operations. Workflow management systems such as ticketing systems, incident tracking systems, or knowledge management systems (all based on some type of database and search capability) can be used to archive and organize information ranging from public monitoring results to vulnerability and vendor security information to incident reports and analysis. The information must be tagged and stored in a way that makes it available to all relevant incident management personnel. Such systems should allow for searching and correlating information. Having a centralized system can reduce duplicate storage and dissemination of information.

These systems can be used to capture a variety of data—from standard responses given to various common questions, to event and incident summaries. Supplemental systems should be used to provide high-priority information across shifts such as electronic or hand-written operations logs or summaries. Operations logs can take the form of blogs, instant messaging, bulletin boards, or whiteboards. Information in operations logs can include

- information about events and incidents that are open, closed, or unresolved
- current advisories and alerts
- current network monitoring alert data

All attempts should be made to ensure that all relevant members of the team can find information about any incident or vulnerability being handled—unless some specific issues with confidentiality, personal privacy, or national security are involved. In that case, access to the information may be limited on a need-to-know basis.

Team Guidance

The intent of this capability is to show that incident management personnel have a well-maintained, complete picture of incident activity and the reports they have received. This is an essential part of managing activities across time shifts, passing information down to incoming personnel, and enabling people to coordinate and communicate, particularly for those incidents that involve weeks or even months of activity.

This capability involves looking for three basic issues to be dealt with—all of which are necessary to meet this capability:

1. Documentation of information related to an incident must be done throughout the incident's lifecycle. This includes analysis, response, and follow-up activities.
2. Information on individual incidents must be available to the team, allowing anyone to pick up the handling of the incident as needed or find out the status of the incident.
3. Workflow management processes and/or mechanisms must be in place to allow for transitioning incidents from one staff member to another, for showing the status of each incident and for providing the storage and correlation of incident and vulnerability data and related artifacts. If shifts exist, this may also require shift handoffs (N/A if there are no shifts). These processes and mechanisms can be digital or not.

References

Regulatory References: None

Guidance References: None

Organization Response

Examples of Evidence Sought

- ❑ Documented workflow management processes or procedures
- ❑ Demonstration of workflow management tools or mechanisms
- ❑ Example incident reports showing analysis, response, and recovery actions have been documented
- ❑ Electronic or manual shift logs or summaries

Scoring Criteria	Yes	No	Evidence
Required			
1.2.4.01 Control: A process and related guidance is in place requiring incident management personnel to document actions	❒	❒	

taken through all phases of handling the incident, including initial characterization through analysis, response, and recovery.			
1.2.4.02 Activity: Incident management personnel document actions taken through all phases of handling the incident, including initial characterization through analysis, response, and recovery.	❒	❒	
1.2.4.03 Activity: Incident and vulnerability data and corresponding artifacts related to incident reports are available to all team members at all times unless exempted by organizational management or policy.	❒	❒	
1.2.4.04 Activity: Workflow management processes and/or tools are used to ensure continuity of incident management operations and appropriate storage, tracking, and sharing of data within the incident management function and other approved personnel.	❒	❒	
1.2.4.05 Activity: Continuity of incident management operations during shift handoffs is ensured.			
Recommended Best Practices			
1.2.4.06 Control: A process and related guidance is in place requiring incident management personnel to document actions taken through all phases of handling the incident including initial characterization through analysis, response, and recovery.	❒	❒	
1.2.4.07 Activity: Incident management personnel document actions taken through all phases of handling the incident including initial characterization through analysis, response, and recovery.	❒	❒	
Institutional and Quality Improvement			
1.2.4.08 Quality: Sample validation that incident reports or data are being documented throughout the lifecycle (i.e., including analysis, response, and recovery phases) is performed.	❒	❒	
1.2.4.09 Quality: Personnel are aware of, knowledgeable of, and consistently follow the procedures, processes, methodologies, and technologies for collecting and using this information.	❒	❒	
1.2.4.10 Quality: A process and criteria exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	

1.2.4.11 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**		❒
Not Applicable		❒	**Not Observed**		❒

Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement

A knowledge management system or database is used to store information collected from public monitoring so that information is not duplicated in emails and is available in searchable manner.

1.2 CORE PROCESSES AND TOOLS

1.2.5 A central repository exists for recording and tracking security events and incidents.

Priority I

Clarification

This capability gauges the existence of a repository (clearinghouse) to collect and archive data on events and incidents reported to the incident management function. Such a repository supports the collection and storage of historical information. This information can then be easily searched for common intruder signatures and attacks, correlated incidents, relevant mitigation and resolution strategies, and historical trends.

This consolidated data can be used as a source for any situational awareness, incident correlation, or other incident analysis (including fusion analysis or retrospective analysis) that may be done. Events are included here because some incidents are only declared after a review of different events reveals a pattern of activity or behavior that indicates an incident. This type of analysis can be essential for identifying "low and slow" attacks and managing such incidents.

A secondary intent of this capability is to gauge whether the right set of information on events and incidents is collected and retained.

In addition, depending on relevant laws and regulations, it might be critical that the right set of information on events and incidents is collected and retained to support LE investigations. Collecting, retaining, and analyzing event and incident information in a way that is acceptable in a court of law is essential to prosecuting criminal activities. If proper methods are not used, organizations may not be able to prosecute due to insufficient, corrupted, or inconclusive data.

Team Guidance

The assessment team should look for evidence that information is retained in an accessible and searchable manner with appropriate access controls and that data is stored commensurate to its classification.

The team should ensure that tools, techniques, and processes exist for collecting, protecting, and appropriately storing the information, as well as for easily accessing and extracting content (e.g., statistics, trends, reports, types of reports, organizations/sites, status) for a variety of needs.

In some organizations with distributed incident management responsibilities, a CSIRT may function more as a coordinator, with individual groups or departments maintaining their own repositories of event and incident data. Even in this case, the CSIRT must be able to access or synthesize that data for the purposes of trending and other analyses.

The mechanisms used to support the central repository can be simple or complex (e.g., email folders, separate files, a spreadsheet, an automated tool or database, customized software), but they do need to meet the organization's needs, be appropriately managed and controlled (like any other critical application or tool), and be able to scale up or adapt to changing conditions. The supporting mechanisms should

- contain fields that include but are not limited to incident type/category/severity, affected sites, systems (IP addresses/hostnames), incident description, and actions taken
- provide functionality to produce incident activity summaries, affected sites lists, action lists, and administrative statistics

- retain event/incident data, at a minimum, as required by the organization for incident reporting
- be documented in up-to-date user guides
- have sufficient backup capability
- be easy to use and adaptable to changing requirements
- be consistent, reliable, interoperable (e.g., can import/export data internally and externally from the organization), and available (backups for data and software, off-site data centers, swaps)
- be developed, documented, and maintained per the organization's lifecycle requirements for software/system development, with full hardware/software support for maintenance available

The controls used to limit access to the incident reporting central repository (see the Required Control indicator for this capability) should include and comply with all applicable security controls such as those recommended in the Access Control family of NIST SP 800-53 Rev 3, but not listed individually here. Other security controls may also apply. Instead of trying to validate the security controls implemented to protect the repository, the team may want to ask whether a security control assessment (or audit) has been conducted on the repository. If it has, team members should review the results of that assessment.

Note that in the absence of specific guidance from local LE, the organization may have to make its best, educated guess or find guidance from its legal representatives on evidence chain of custody and other LE requirements. The assessment team may need to judge whether an organization has done all that it can to create a reasonable set of policies, procedures, and guidelines to perform this function.

References

Regulatory References:

General Records Schedule (GRS) 24—Information Technology Operations and Management Records [NARA 2010]

> "7. Computer Security Incident Handling, Reporting and Follow-up Records. Destroy/delete three years after all necessary follow-up actions have been completed"

Guidance References:

NIST SP 800-61 Rev 2 *Computer Security Incident Handling Guide* [Cichonski 2012]

> [p 30-31]
>
> "An incident response team that suspects that an incident has occurred should immediately start recording all facts regarding the incident.[10] A logbook is an effective and simple medium for this,[11] but laptops, audio recorders, and digital cameras can also serve this purpose.[12] Documenting system events, conversations, and observed changes in files can lead to a more efficient, more systematic, and less error-prone handling of the problem. […]

[10] Incident handlers should log only the facts regarding the incident, not personal opinions or conclusions. Subjective material should be presented in incident reports, not recorded as evidence.

[11] If a logbook is used, it should be bound, and the incident handlers should number the pages, write in ink, and leave the logbook intact (i.e., do not rip out any pages).

[12] Consider the admissibility of evidence collected with a device before using it. For example, any devices that are potential sources of evidence should not, themselves, be used to record other evidence.

Sec 2.3.4.2 Law Enforcement
The incident response team should become acquainted with its various law enforcement representatives before an incident occurs to discuss […] what evidence should be collected, an how it should be collected.

Sec 3.2.5 Incident Documentation
An incident response team that suspects that an incident has occurred should immediately start recording all facts regarding the incident. […]
The incident response team should maintain records about the status of incidents, along with other pertinent information. […]

Sec 3.3.2 Evidence Gathering and Handling
[…]In such cases, it is important to clearly document how all evidence, including compromised systems, has been preserved. Evidence should be collected according to procedures that meet all applicable laws and regulations that have been developed from previous discussions with legal staff and appropriate law enforcement agencies so that any evidence can be admissible in court. In addition, evidence should be accounted for at all times; whenever evidence is transferred from person to person, chain of custody forms should detail the transfer and include each party's signature.

Sec 3.4.2 Using Collected Incident Data

Over time, the collected incident data should be useful in several capacities. […] A study of incident characteristics may indicate systemic security weaknesses and threats, as well as changed in incident trends.

Sec 3.4.3 Evidence Retention
Prosecution. If it is possible that the attacker will be prosecuted, evidence may need to be retained until all legal actions have been completed. […]
Data Retention. Most organizations have data retention policies that state how long certain types of data may be kept. […]"

[NIST SP 800-61 Rev 2] Section 3.3.2 presents more information about evidence.[13]

"The incident response team should maintain records about the status of incidents, along with other pertinent information.[14] Using an application or a database, such as an issue tracking system, helps ensure that incidents are handled and resolved in a timely manner. The issue tracking system should contain information on the following:

- The current state of the incident (new, in progress, forwarded for investigation, resolved, etc.)
- A summary of the incident
- Indicators related to the incident
- Other incidents related to this incident
- Actions taken by all incident handlers on this incident
- Chain of custody, if applicable
- Impact assessments related to the incident
- Contact information for other involved parties (e.g., system owners, system administrators)

[13] NIST SP 800-86, *Guide to Integrating Forensic Techniques Into Incident Response,* provides detailed information on establishing a forensic capability, including the development of policies and procedures.

[14] [NIST SP 800-61 Rev 2] Appendix B contains a suggested list of data elements to collect when incidents are reported. Also, the CERT®/CC document *State of the Practice of Computer Security Incident Response Teams (CSIRTs)* provides several sample incident reporting forms. The document is available at https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6571 [Killcrece 2003a].

- A list of evidence gathered during the incident investigation
- Comments from incident handlers
- Next steps to be taken (e.g., rebuild the host, upgrade an application)[15]

The incident response team should safeguard incident data and restrict access to it because it often contains sensitive information"

NIST SP 800-53 Rev 4 *Security and Privacy Controls for Federal Information Systems and Organizations* [NIST 2013]

"IR-5 INCIDENT MONITORING

Control: The organization tracks and documents information system security incidents.

Supplemental Guidance: Documenting information system security incidents includes, for example, maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports."

Expectations *for Computer Security Incident Response* [NWG 1998]

"Archiving services

- Central logging service […]
- - Records of security incidents handled will be kept. […]"

Organization Response

Examples of Evidence Sought

- ❑ Demonstrations or observations of repository mechanisms
- ❑ Sample records or reports from a central repository
- ❑ Documentation or demonstration of access controls and/or encryption on the repository
- ❑ Backup systems or mechanisms
- ❑ Schedules for backing up or archiving reports
- ❑ Alternate sites for archiving records
- ❑ Results of security control assessments or audits conducted on the repository
- ❑ Encryption techniques to store data in the repository or archive
- ❑ Documents or input from local LE on what information is needed and other requirements

[15] The Trans-European Research and Education Networking Association (TERENA) has developed RFC 3067, *TERENA's Incident Object Description and Exchange Format Requirements* (http://www.ietf.org/rfc/rfc3067.txt). The document provides recommendations for what information should be collected for each incident. The Internet Engineering Task Force (IETF) Extended Incident Handling Working Group (https://datatracker.ietf.org/wg/inch/charter/) created an RFC that expands on TERENA's work—RFC 5070, *Incident Object Description Exchange Format* (http://www.ietf.org/rfc/rfc5070.txt).

❑ Repository (and backup) of event and incident data—in soft and/or hard copy—that supports chain of custody requirements			
Scoring Criteria	Yes	No	Evidence
Required			
1.2.5.01 Control: There is an organizational requirement to centrally collect events and incident reports.	❒	❒	
1.2.5.02 Control: There is a policy or guidance for data retention.	❒	❒	
1.2.5.03 Control: Guidelines and processes exist for secure collection, handling, transmission, storage, and destruction of event and incident data.	❒	❒	
1.2.5.04 Control: Access controls on the central repository limit access to authorized incident management personnel.	❒	❒	
1.2.5.05 Control: Personnel are appropriately and consistently trained in the processes and relevant technology.	❒	❒	
1.2.5.06 Activity: All the event and incident reports from the organization are retained in a central repository (either in hard copy or electronic form) in accordance with organizational guidelines.	❒	❒	
1.2.5.07 Activity: Designated incident information and supporting materials are collected in a forensically sound manner to support LE to the extent required according to policy.	❒	❒	
1.2.5.08 Activity: The central repository is backed up.	❒	❒	
Recommended Best Practices			
1.2.5.09 Activity: All electronic archived reports are encrypted (using FIPS 140-2 compliant cryptography).	❒	❒	
1.2.5.10 Activity: The backup for the central repository is at an off-site location.	❒	❒	
1.2.5.11 Activity: Periodic reviews are conducted to ensure the security of data repositories.	❒	❒	
1.2.5.12 Activity: Backups are periodically checked to verify restoration can occur.	❒	❒	

Institutional and Quality Improvement			
1.2.5.13 Control: Documented procedures exist for archiving, retiring, and destroying records.	❒	❒	
1.2.5.14 Quality: Personnel are aware of, knowledgeable of, and consistently follow the procedures for this activity.	❒	❒	
1.2.5.15 Quality: Secure repository is reviewed at least annually to ensure security is adequate.	❒	❒	
1.2.5.16 Quality: A process and criteria exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	
1.2.5.17 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒
Not Applicable		❒	**Not Observed**	❒

Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement
• Off-site archiving is easier to achieve with a centralized database or knowledge base for events and incidents but may be more difficult if the data is distributed. • Encrypt all retained information (which would also help meet other capabilities associated with maintaining the confidentiality of sensitive information).

- Track retention rates to ensure guidelines are met.
- Implement automated tools that help in the correlation of data and analysis.
- Use criteria such as verification of retention timeframes and adequacy of the secure repository to evaluate how well this activity is performed and the quality of its artifacts.
- Have documentation from LE that describes LE information requirements. (This serves as an excellent reference but may not always be available.)
- Verify that the activity is being done correctly. It takes some time, but collecting and retaining information in a forensically approved way may be critical to supporting the evidence chain of custody.

1.2 CORE PROCESSES AND TOOLS

1.2.6 Security events and incidents are categorized and prioritized according to organizational guidance.

Priority II

Clarification

The intent of this capability is to show that the organization has a formal, documented process for sorting, categorizing, and prioritizing security events and incidents, as well as other types of incoming information. Having a defined process for handling all information that is received through an initial entry point is an essential element of an incident management capability.

The categorization and prioritization of information are two important functions of what is sometimes referred to as the *triage* process, which typically also includes correlation and assignment of incoming reports and information to the appropriate personnel for further action.[16] Triage allows for an initial assessment of incoming information and queues it for further handling.

The categorization of events and incidents uses predefined criteria to identify the incoming information. The categories and criteria are developed (and updated as needed) by the organization. Events and incidents can be categorized in a variety of ways, such as the attack vector or method used (e.g., probe/scan, unpatched vulnerability, password cracking, social engineering or phishing attack), the impact (e.g., denial of service, compromised account, data leakage), the scope (e.g., number of systems affected), whether the attack was successful versus unsuccessful, or other factors. Since incidents often involve more than one method or impact, the incident categorization should not be limited to only a single category but rather be tagged with multiple categories as appropriate. For example, an incident may involve unauthorized access to a compromised account that was used to install malicious code that later caused a denial of service.

Note that the concept of "incident categories" has been replaced with "attack vectors" in the revised NIST SP 800-61 Rev 2 *Computer Security Incident Handling Guide* [NIST 2012].

Team Guidance

Organizations should maintain their own list of incident categories and prioritization criteria to execute their own incident management mission.

The categorization (and prioritization) of incidents is closely coupled with the organization's incident reporting guidelines and with the tools or database the organization uses to track reported incidents. Cross-check this capability with Response capabilities 4.1.1, 4.1.2, and 4.1.3 to determine whether the organization's incident reporting guidelines provide any guidance on incident categories (or priorities) and with Prepare capability 1.2.5 to determine whether the organization's central incident repository provides criteria for categorizing and prioritizing incidents.

References

Regulatory References:

[16] For further information about the triage process, see Section 4.2.4 "Triage Events" in *Defining Incident Management Processes for CSIRTs: A Work in Progress* (CMU/SEI-2004-TR-015) [p 112-127], https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=7153 [Alberts 2004].

None

Guidance References:

NIST SP 800-61 Rev 2 *Computer Security Incident Handling Guide* [Cichonski 2012]

> "Sec 3.2.6 Incident Prioritization
> [p 32-33]
>
> Prioritizing the handling of the incident is perhaps the most critical decision point in the incident handling process. Incidents should not be handled on a first-come, first-served basis as a result of resource limitations. Instead, handling should be prioritized based on the relevant factors, such as the following:
>
> - Functional Impact of the Incident.
> - Information Impact of the Incident.
> - Recoverability from the Incident. […] The team should prioritize the response to each incident based on its estimate of the business impact caused by the incident and the estimated efforts required to recover from the incident."

[indirect]

NIST SP 800-61 Rev 2 *Computer Security Incident Handling Guide* [Cichonski 2012]

> "Sec 3.2.1 Attack Vectors
> [p 25-26]
>
> Incidents can occur in countless ways, so it is infeasible to develop step-by-step instructions for handling every incident. Organizations should be generally prepared to handle any incident but should focus on being prepared to handle incidents that use common attack vectors. Different types of incidents merit different response strategies. The attack vectors listed below are not intended to provide definitive classification for incidents; rather, they simply list common methods of attack, which can be used as a basis for defining more specific handling procedures.
>
> - External/Removable Media […]
> - Attrition […]
> - Web […]
> - Email […]
> - Impersonation […]
> - Improper Usage […]
> - Loss of Theft of Equipment […]
> - Other […]"

Organization Response

Examples of Evidence Sought

- ❑ Documented criteria for incident categorization (or attack vectors)
- ❑ Documented criteria for incident prioritization
- ❑ Other documentation or guidance that provides criteria for incident categorization or prioritization (e.g., CSIRT CONOPS, incident reporting guidelines or requirements)

- ❑ Automated tools (incident reporting form, incident tracking system) that use predefined incident categories
- ❑ Observation of incident management personnel categorizing incoming incidents

Scoring Criteria	Yes	No	Evidence
Required			
1.2.6.01 Control: Documented criteria exist for categorizing and prioritizing events and incidents.	❒	❒	
1.2.6.02 Control: Documented process exists for categorizing and prioritizing events and incidents.	❒	❒	
1.2.6.03 Control: Documented guidelines, thresholds, or criteria exist for when to escalate events/incidents.	❒	❒	
1.2.6.04 Activity: Security events and incidents are categorized using predefined criteria.	❒	❒	
1.2.6.05 Activity: Security events and incidents are prioritized using predefined criteria.	❒	❒	
Recommended Best Practices			
1.2.6.06 Control: The organization's incident repository uses predefined incident categories.	❒	❒	
1.2.6.07 Control: The organization's centralized incident repository provides the option to assign more than one incident category to an incident.	❒	❒	
1.2.6.08 Control: Guidance is provided on categorizing and prioritizing events and incidents that cannot be categorized or prioritized using the predefined criteria.	❒	❒	
1.2.6.09 Control: Guidance is provided on the process for changing the priority (escalate or de-escalate) of incidents, as needed.	❒	❒	
1.2.6.10 Activity: Automated tools (including incident reporting tools) use predefined criteria to categorize and prioritize security events and incidents.	❒	❒	
Institutional and Quality Improvement			
1.2.6.11 Control: Documented procedures exist for determining the category and priority of events and incidents.	❒	❒	

1.2.6.12 Quality: Personnel are aware of, knowledgeable of, and consistently follow the procedures for this activity.	❒	❒	
1.2.6.13 Quality: A process and criteria exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	
1.2.6.14 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒
Not Applicable		❒	**Not Observed**	❒

Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement
None

1.2 CORE PROCESSES AND TOOLS

1.2.7 An insider threat program exists within the organization. **Priority I**

Clarification

Increasingly, organizations are recognizing the need to counter insider threats and are doing it through specially focused teams. In January 2011, the Federal OMB released memorandum M-11-08, *Initial Assessments of Safeguarding and Counterintelligence Postures for Classified National Security Information in Automated Systems*. It announced the evaluation of the insider threat safeguards of government agencies. This action by the Federal government highlights the pervasive and continuous threat to government and private industry from insiders, as well as the need for programs that mitigate this threat. In October 2011, the U.S. President Barack Obama signed Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information.*

This capability focuses on ensuring that an insider threat program has been established and institutionalized. Such a program concentrates on developing specific organizational policies, procedures, practices, processes, and supporting guidance to deter, detect, and mitigate actions by employees who may represent a threat to national security. These threats encompass: potential espionage, violent acts, and unauthorized disclosure of information. Employees include not just staff but contractors, suppliers, business partners, and collaborators.

In general the elements or components of such a program include the capability to gather, integrate, and centrally analyze and respond to key threat-related information; monitor employee use of sensitive networks; provide the workforce with insider threat awareness training; and protect the civil liberties and privacy of all personnel according to established Federal laws, regulations, and organizational requirements.

Threat-related information to be collected and analyzed includes both technical and behavioral observables. Technical observables include but are not limited to such categories and examples as

- physical (facility access records; printer, copier, and facsimile [FAX] machine access; asset location and tagging; access to removable media)
- host-based/single-user workstation (removable media usage, data addition/modification/exfiltration, data and network traffic tagging, object/file access success/failure)
- network-based (intrusion detection logs, network resource access success/failure, data loss prevention logs, data exfiltration, email monitoring, web activity monitoring, remote access logs)
- configuration management (device configuration and settings logs; device software installation logs; unauthorized software or application usage)

Behavioral observables include but are not limited to such categories and examples as

- individual personal, financial, or professional/work stressors
- organizational actions, events, and conditions
- physical security (facility access logs, badging records, access attempts)
- personnel Management/HR (performance improvement plans, sanctions, workplace violence)

- concerning behaviors of employees (alcohol/drug usage, co-workers' reports of suspicious or aggressive behavior, security violations)
- counterintelligence (foreign contact risk, suspicious travel, financial issues, arrest)

Such a program should also include defined processes and guidance for confidential reporting, policies, and procedures that facilitate and support execution of the program. And it should define acceptable behaviors and consequences of non-compliance such as firing, suspension, counseling, or referral to other organizations like LE or inspector general (IG). Program components should ensure that policies and procedures are in place for employee monitoring, and include performing background checks before hiring and following a standard termination procedure that ensures all types of access (account, remote, physical) are removed and employees are reminded of any signed NDAs, IP agreements, or acceptable use policies.

To be successful a program must be enterprise in nature involving components from HR, Legal, Facilities, Security, IT, business and line units, and senior management. An Insider Threat Team should be established to review and analyze observables and handle detected incidents.

Team Guidance

An insider threat program is an enterprise-wide program with an established vision and defined roles and responsibilities for those involved. All individuals participating in the program must receive specialized awareness training. The program must have criteria and thresholds for conducting inquiries, referring to investigators, and requesting prosecution. Inquiries must be controlled by a process to ensure privacy and confidentiality because the team will be a trusted group for monitoring and resolution. Most importantly, the program must have management's support to be successful. The team should look for evidence that each one of those issues is being addressed.

The insider threat program may be a stand-alone program or part of a larger security or incident management (response) program. It is acceptable if it is built as part of such a larger program, as long as the minimum standards are met. There is no standard place for the authority of this program to reside. It may be within general security or risk management areas.

Team members should look for evidence that the components are not only in place but are institutionalized and known throughout the organization. They should also look for evidence that shows the program involves components from across the enterprise.

References

Regulatory References:

Executive Order 13587—*Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*

> "b) implement an insider threat detection and prevention program consistent with guidance and standards developed by the Insider Threat Task Force established in section 6 of this order
>
> Presidential MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES
>
> SUBJECT: National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs
>
> This Presidential Memorandum transmits the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs (Minimum Standards) to provide direction and guidance to promote the development of effective insider threat programs

within departments and agencies to deter, detect, and mitigate actions by employees who may represent a threat to national security. These threats encompass potential espionage, violent acts against the Government or the Nation, and unauthorized disclosure of classified information, including the vast amounts of classified data available on interconnected United States Government computer networks and systems.

The Minimum Standards provide departments and agencies with the minimum elements necessary to establish effective insider threat programs. These elements include the capability to gather, integrate, and centrally analyze and respond to key threat-related information; monitor employee use of classified networks; provide the workforce with insider threat awareness training; and protect the civil liberties and privacy of all personnel.

The resulting insider threat capabilities will strengthen the protection of classified information across the executive branch and reinforce our defenses against both adversaries and insiders who misuse their access and endanger our national security."

Guidance References:

NIST 800-53 Rev. 4 *Security and Privacy Controls for Federal Information Systems and Organizations* [NIST 2013]

"PM-12 Insider Threat Program

Control: The organization implements an insider threat program that includes a cross-discipline insider threat incident handling team.

Supplemental Guidance: Insider threat programs can leverage the existence of incident handling teams organizations may already have in place, such as computer security incident response teams. Human resources records are especially important in this effort, as there is compelling evidence to show that some types of insider crimes are often preceded by nontechnical behaviors in the workplace (e.g., ongoing patterns of disgruntled behavior and conflicts with coworkers and other colleagues). These precursors can better inform and guide organizational officials in more focused, targeted monitoring efforts. The participation of a legal team is important to ensure that all monitoring activities are performed in accordance with appropriate legislation, directives, regulations, policies, standards, and guidelines."

Organization Response

Examples of Evidence Sought

- ❑ Organizational insider threat program or related guidance, policies, and practices
- ❑ An insider threat incident response plan
- ❑ Training and awareness materials showing education about insider threat crimes, issues, policies, and practices
- ❑ Training records showing attendance on modules regarding insider threat and refreshers
- ❑ Establishment of an insider threat operational team to review and analyze observables
- ❑ Demonstration of tools and mechanisms for collecting and analyzing observables
- ❑ Case records of insider incidents that were detected and resolved or mitigated
- ❑ Evidence of an employee monitoring program
- ❑ Policies and procedures indicating standard hiring and termination processes that meet the required standards

❑ HR or Legal artifacts such as NDAs, IP agreements, or acceptable use documents; Termination or hiring checklists; documentation of consequences of non-acceptable behavior			
Scoring Criteria	Yes	No	Evidence
Required			
1.2.7.01 Control: An organizational insider threat program has been established that meets minimum standards and practices defined by the organization or relevant standards and regulations.	❒	❒	
1.2.7.02 Control: A training and awareness program describing insider threats, crimes, and relevant procedures and practices has been established and is executed on a regular basis.	❒	❒	
1.2.7.03 Control: A process and mechanism for confidential reporting of suspected insider malicious or suspicious behavior is established.	❒	❒	
1.2.7.04 Control: A process and mechanism for monitoring employee access to and activity on relevant networks is established. This includes • end-user monitoring • privileged access monitoring • terminated or soon to be terminated employee monitoring • insider threat team monitoring (i.e., who is ensuring the insider threat team is operating in a trusted manner) • remote access monitoring	❒	❒	
1.2.7.05 Activity: Technical and behavioral observables or indicators are collected and analyzed to detect and respond to insider threats.	❒	❒	

1.2.7.06 Activity: Data aggregation tools are installed, and organizations collect and correlate, for example, the following types of events: • firewall logs • unsuccessful login attempts • IDS/intrusion prevention system (IPS) logs • web proxies • AV alerts • change management	❒	❒	
1.2.7.07 Activity: Detected insider threat activity is mitigated and referred to appropriate organizational components for handling.	❒	❒	
1.2.7.08 Activity: Handling of employees suspected of or caught performing malicious insider actions is done while still protecting their civil liberties and privacy according to relevant laws, regulations, and guidance, and in accordance with organizational policy and procedures.	❒	❒	
Recommended Best Practices			
1.2.7.09 Control: An organizational insider threat council including representatives from HR, Legal, IT, Security, and senior management is established to provide governance for the program.	❒	❒	
1.2.7.10 Control: An insider threat program team is established to perform the operational duties of the program including reviewing and analyzing observables and mitigating identified incidents.	❒	❒	
1.2.7.11 Control: A baseline of network activity has been established.	❒	❒	
1.2.7.12 Activity: Role-based training for organizational employees on insider threat issues and practices is performed, including those who perform insider threat program duties.	❒	❒	
1.2.7.13 Activity: Tagging and monitoring of movement, revision, or deletion of key critical data and IP is performed.	❒	❒	

1.2.7.14 Activity: Data aggregation tools are installed, and organizations collect and correlate, at a minimum, the following types of events: • firewall logs • unsuccessful login attempts • IDS/IPS logs • web proxies • AV alerts • change management			
Institutional and Quality Improvement			
1.2.7.15 Quality: Personnel are aware of, knowledgeable of, and consistently follow the procedures, processes, methodologies, and technologies for collecting and using this information.	❒	❒	
1.2.7.16 Quality: A process and criteria exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	
1.2.7.17 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒	
Not Applicable		❒	**Not Observed**	❒	
Evidence Collected					
Document Review		Interviews		Direct Observation	
Notes					

Suggestions for Improvement

- Organizations should create monitoring policies and procedures before institutionalizing any monitoring program. Employees should be informed that their use of any information system is monitored. This is typically done through login banners and security awareness training provided to users before using a system and through annual refreshers. Organizations should consult legal counsel before implementing any monitoring program to ensure they meet all legal requirements and disclosures.
- Implement secure backup and recovery systems and processes.
- Implement strict password and account management policies and practices.
- Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.

PROTECT: SECTION 2 OF INCIDENT MANAGEMENT CAPABILITIES

The mission of Protect is to adequately protect and secure critical organizational data and assets, including the computing infrastructure of the groups performing incident management capabilities for their organization, in response to current risk, threats, and attacks, while handling information in a timely, secure fashion.

Protect focuses on efforts to

- assess the security posture of the computing infrastructure by performing tasks such as proactive scanning and network monitoring, and by performing security assessments and RAs after obtaining appropriate management approvals
- implement changes to the computing infrastructure to stop or mitigate an ongoing incident, or to stop or mitigate the potential exploitation of a vulnerability in the hardware or software infrastructure
- pass off to the Detect process any information about ongoing events or incidents, discovered vulnerabilities, or other security-related events
- implement infrastructure protection improvements resulting from incident postmortem reviews or other process improvement mechanisms

An incident management function has a role in the protection of organizational networks by helping to prevent incidents from occurring, as well as enabling detection and containment of incidents that do occur. This function can take the form of providing the Protect capabilities directly or providing guidance, recommendations, and assistance to those who perform these capabilities.

For instance, information can be provided to constituents about recommended security best practices, configuration guidelines, filtering policies, vulnerability patching and remediation strategies, general security awareness training, and other activities. Information can also be provided on proactive methods for containing or mitigating incidents by making changes within the infrastructure.

Helping to fortify these systems and networks decreases the potential for successful attacks against the organization's infrastructure and helps to contain and reduce any impact on organizational goals, objectives, and operations. Interfaces should be established with other parts of the organization (internal and external[17]) that are providing security operations management activities involved in the Protect process.[18] Information on configuration management, patch management, and change management activities should be shared across this interface.

[17] An external interface might be with a managed security service provider, for example.

[18] These interfaces should be documented as outlined in capability 1.1.4.

Within the Protect category, the subcategories and their capabilities include the following:

2.1. **Risk Assessment**[19]—Risk assessments are used to measure the computer security posture of information systems and computer networks. This category also includes vulnerability scanning and assessment capabilities.

2.1.1. Security risk assessments (RAs) are performed on the constituents' organization.

2.1.2. The constituents get help correcting problems identified through security risk assessment (RA) activities.

2.2. **Prevention**—Incident management personnel play a vital role in the in-depth protection of organizational systems, networks, and information from malicious activity.

2.2.1. The organization has an institutionalized malware prevention program.

2.3. **Operational Exercises for Incident Management—**Mock exercises test the response plans and reactions of incident management personnel and the organization to various incident and vulnerability scenarios.

2.3.1. Operational exercises are conducted to assess the IM function of the organization.

2.4. **Training and Guidance**—Incident management personnel must be knowledgeable about organizational network configurations to assist with "hardening" systems and correcting vulnerabilities identified in network configurations. The intent is that incident management personnel will participate in efforts to communicate computer security knowledge and awareness to the community it serves.

2.4.1. Guidance is provided to constituents on best practices for protecting their systems and network.

2.4.2. Constituents are provided with security education, training, and awareness (ETA).

2.5. **Vulnerability Management**—This positive control system participates in identifying new system vulnerabilities and notifies the appropriate parts of the organization to enable the application of effective countermeasures. Incident management personnel monitor constituent compliance with vulnerability recommendations and prevention strategies, as well as provide technical support as required.

2.5.1. A patch management and alert program exists.

2.5.2. Proactive vulnerability assessment is performed on constituent networks and systems.

2.5.3. Constituents receive help to correct problems identified by vulnerability assessment activities.

[19] An example assessment tool is the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Method developed at the SEI [SEI 2003].

2.1 RISK ASSESSMENT

2.1.1 Security risk assessments (RAs) are performed on the constituents' organization.

Priority I

Clarification

The intent of this capability is to ensure that security RAs are performed periodically and the results are used to improve the security posture of the organization. Periodic security RAs are required by FISMA (see Regulatory References for this capability).[20]

Response to this capability determines whether security RAs are performed on the constituents' organization, including its systems and networks. (Capability 5.6.5 addresses security RAs on incident management systems.) Security RAs are used to identify weaknesses and vulnerabilities in the infrastructure and constituent security practices before those weaknesses and vulnerabilities can be exploited. Security RA allows potential problem areas to be mitigated proactively, increasing the overall security of the organization as well as its systems and networks. Incident management personnel may or may not be involved in performing the security RAs, but they should have access to the results, even if the security RAs are conducted by third parties.

The scope of this capability is broader than an organization's Certification and Accreditation (C&A) activities, which focus on addressing security risks to information systems. C&A is a systematic procedure for evaluating, describing, testing, and authorizing an information system prior to or after it is in operation to ensure that it operates within an acceptable level of risk. C&A activities are limited to an organization's information systems; they do not assess organizational security risks. As a result, C&A, by itself, does not address the full extent of this capability.

Team Guidance

The assessment team should determine which methods and tools are used by the organization to perform security RAs and analyze the resulting outputs. This determination can be done through interviews with organizational staff or by observing them.

The team should look for evidence that

- security RA policies (and/or procedures) are documented as part of the organization's information security program as required by relevant standards, guidelines, or policies
- the risks are mitigated once identified (e.g., by changes in policies and procedures, changes to the infrastructure, or the implementation of new controls or security tools)

The team should look for evidence that the security RA process is evaluated periodically and that appropriate improvements are made. Examples of evidence include evaluation results, lessons learned reports, and improvement plans for the security RA process, as well as any changes or updates to the security RA process, methods, and tools.

In the following Recommended Best Practices section, it states that even if incident management personnel never actually provide assistance, they should have access to the lessons learned from security RAs. That access can help them stay informed about the current security posture of the

[20] The term "periodic" means that the security RAs are routine and conducted at a frequency defined by the organization (per NIST 800-53).

organization and improve the incident management function. The team should look for evidence that results are being provided to incident management personnel.

This capability might be outsourced or handled by another part of the organization. In that case, this capability should be applied to that group and its activities. If the parent organization determines this capability is not within the scope of its incident management processes, it can also be marked not applicable.

For the "Required" indicators listed for this capability, the organization should have some guidance on how it protects its sensitive risk data (e.g., encryption, access control lists [ACLs], special physical storage). If the organization doesn't have any such guidelines, it should have a policy stating that protection of risk data is not a concern for the organization.

References

Regulatory References:

FISMA Sec 3544 *Federal agency responsibilities*(b)(1) [OLRC 2003]

> "(b) AGENCY PROGRAM […]
>
> (1) periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency."

FIPS 199 *Standards for Security Categorization of Federal Information and Information Systems* [NIST 2004]

> "FIPS Publication 199 addresses the first task cited—to develop standards for categorizing information and information systems."

Guidance References:

NIST SP 800-30 Rev 1 *Guide for Conducting Risk Assessments* [JTFTI 2012]

> "The purpose of SP 800-30 is to provide guidance for conducting RAs of Federal information systems and organizations, amplifying the guidance in SP 800-39. RAs, carried out at all three tiers in the risk management hierarchy, are part of an overall risk management process—providing senior leaders/executives with the information needed to determine appropriate courses of action in response to identified risks. […]"

NIST SP 800-39 *Managing Information Security Risk: Organization, Mission, and Information System View* [NIST 2011]

> [p 6]
>
> "Risk management is a comprehensive process that requires organizations to: (i) *frame* risk (i.e., establish the context for risk-based decisions); (ii) *assess* risk; (iii) *respond* to risk once determined; and (iv) *monitor* risk on an ongoing basis using effective organizational communications and a feedback loop for continuous improvement in the risk-related activities of organizations."

NIST SP 800-53 Rev 4 *Security and Privacy Controls for Federal Information Systems and Organizations* [NIST 2013]

> "RA-3 Risk Assessment
> The organization: […]
>
> a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;

b. Documents risk assessment results in [Selection: security plan; risk assessment report; [Assignment: organization-defined document]];
c. Reviews risk assessment results [Assignment: organization-defined frequency]; and
d. Disseminates risk assessment results to [*Assignment: organization-defined personnel or roles*] and;
e. Updates the risk assessment [Assignment: organization-defined frequency] […]"

NIST 800-37 Rev. 1: *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Lifecycle Approach* [NIST 2010]

"The purpose of this publication is to provide guidelines for applying the Risk Management Framework to Federal information systems. […]"

International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 31000, *Risk management—Principles and guidelines*

ISO/IEC 31010, *Risk management—Risk assessment techniques*

ISO/IEC 27005, *Information technology—Security techniques—Information security risk management systems*

A Step-By-Step Approach on How to Set Up A CSIRT [ENISA 2006]

"Generating Alerts, Warnings and Announcements…

Risk assessment & impact analysis

There are several methods for determining the risk and impact of a (potential) vulnerability. Risk is defined as the potential chance that the vulnerability can be exploited. There are several important factors […]"

Organization Response

Examples of Evidence Sought

- ❑ Copy of security RA program, policy, procedures, or guidance
- ❑ Copies of security RA results and improvement/mitigation actions
- ❑ List of security RA types and providers
- ❑ Letter, email, or policy giving approval for security RAs to be conducted
- ❑ Mechanisms for requesting assistance
- ❑ Mechanisms for providing security RA results and information to the requestor

Scoring Criteria	Yes	No	Evidence
Required			
2.1.1.01 Prerequisite: Management has given approval for conducting security RAs on the constituents' organization.	❒	❒	
2.1.1.02 Control: Documented policy or guidance exists for conducting security RAs.	❒	❒	

2.1.1.03 Control: Personnel are trained appropriately on the process, methods, and supporting technologies used to provide, conduct, or contract for security RAs.	❒	❒	
2.1.1.04 Activity: Security RAs are performed on the constituents' organization.	❒	❒	
2.1.1.05 Activity: Identified risks are mitigated or addressed.	❒	❒	
2.1.1.06 Activity: Security RA results are tracked and recorded.	❒	❒	
2.1.1.07 Activity: Security RA results are provided to the organization.	❒	❒	
2.1.1.08 Activity: Security RA results are archived in a secure and protected manner according to organizational guidelines.	❒	❒	
2.1.1.09 Activity: Security RA results are communicated in a secure and protected manner according to organizational guidelines.	❒	❒	
Recommended Best Practices			
2.1.1.10 Activity: Lessons learned from security RAs are incorporated into security RA processes, training, and testing.	❒	❒	
2.1.1.11 Control: Guidelines exist for requesting security RA assistance from authorized security RA personnel or providers.	❒	❒	
2.1.1.12 Activity: Incident management personnel have access to the results of security RAs if they do not actually perform them.	❒	❒	
2.1.1.13 Activity: Technical assistance for performing security RAs is provided to the constituents if needed.	❒	❒	
2.1.1.14 Activity: A list of security RA providers and the type of assessments they perform (e.g., Control Objectives for Information and related Technology [COBIT], OCTAVE®) is collected, maintained, and updated if third-party providers perform security RAs for the organization.	❒	❒	
2.1.1.15 Activity: Security RA results are provided to incident management personnel.	❒	❒	

Institutional and Quality Improvement			
2.1.1.16 Control: Documented procedures exist for either conducting the security RA (e.g., COBIT, OCTAVE) or contracting with a third party to conduct it, and for analyzing the security RA results.	❒	❒	
2.1.1.17 Quality: Personnel are aware of, knowledgeable of, and consistently follow the applicable procedures, processes, methodologies, and technologies for performing these activities.	❒	❒	
2.1.1.18 Quality: A process and criteria exist for evaluating the quality of security RA performance and artifacts.	❒	❒	
2.1.1.19 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒
Not Applicable		❒	**Not Observed**	❒

Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement

- Implement guidelines for determining when and how prior notification of the security RA should be made to incident management operations so the assessment will not trigger false alarms or interfere with other incident management operations (situational awareness).

- Implement quality assurance (QA) checks on the type of security RA method and the information produced to ensure that it is complete, timely, accurate, clear, up to date, useful, and meets any organization, institutional, or legal compliance guidelines.
- Train constituent personnel and security RA personnel on the types of security RAs available, security RA providers, how to choose the most appropriate type of security RA, and specific security RA methods. Incident management personnel providing this service should be knowledgeable in the appropriate security RA methods.

2.1 RISK ASSESSMENT

2.1.2 The constituents get help correcting problems identified through security risk assessment (RA) activities.

Priority II

Clarification

This capability focuses on providing constituents with the needed technical recommendations, guidance, and support to help correct the security problems and vulnerabilities, and mitigate the risks identified during a security RA. Depending on the level and set of incident management services provided, this assistance could

- consist of offering organizational and technical mitigation strategies and recommendations
- include working with the appropriate personnel to implement changes to constituent policies and procedures
- take the form of hands-on configuration where incident management personnel make the corrections or work with the appropriate system or network owner to make the changes

Team Guidance

If another part of the organization conducts security RAs and implements appropriate mitigation strategies and recommendations, incident management personnel must be able to access the results of the security RAs. The part of the organization that conducts security RAs and helps with mitigation is the group that is assessed.

Security risk mitigation involves making changes in the organization and its infrastructure to contain, eradicate, or fix actual or potential malicious activity or to address organizational conditions that could lead to malicious activity. Such actions might include

- making changes in constituent policies and procedures to correct weaknesses identified during the security RA
- making changes in filters on firewalls, routers, or mail servers to prohibit malicious packets from entering the infrastructure
- updating IDS or AV signatures to identify and contain new threats
- installing patches for vulnerable software

Security risk mitigation strategies or recommendations should implement defense in depth and other best security practices to ensure that the organization's security risk is within an acceptable tolerance. The resulting in-depth defenses limit the opportunities for attacks, threats, and vulnerabilities to be successful in breaching security. The constituency's implementation of mitigation strategies or recommendations should be controlled using the constituency's configuration management, patch management, and change management processes.

References

Regulatory References:

FISMA Sec 3544 *Federal agencies responsibilities* (b)(6) [OLRC 2003]

"(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] that includes— […]
(6) a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency"

OMB Cir A-130 *Memorandum for Heads of Executive Departments and Agencies* App III Sec A.5.a.

"Correction of Deficiencies. Agencies shall correct deficiencies which are identified through the reviews of security for systems and major applications described above."

Guidance References:

NIST SP 800-30 Rev 1 *Guide for Conducting Risk Assessments* [JTFTI 2012]

"The purpose of SP 800-30 is to provide guidance for conducting RAs of Federal information systems and organizations, amplifying the guidance in SP 800-39. RAs, carried out at all three tiers in the risk management hierarchy, are part of an overall risk management process—providing senior leaders/executives with the information needed to determine appropriate courses of action in response to identified risks. In particular, this document provides guidance for carrying out each of the steps in the *risk assessment process* (i.e., preparing for the assessment, conducting the assessment, communicating the results of the assessment, and maintaining the assessment) and how RAs and other organizational risk management processes complement and inform each other. […]"

NIST 800-37 Rev.1: *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Lifecycle Approach* [NIST 2010]

"The purpose of this publication is to provide guidelines for applying the Risk Management Framework to Federal information systems. […]"

NIST 800-39 *Managing Information Security Risk: Organization, Mission, and Information System View* [NIST 2011]

"NIST SP 800-39 is the flagship document in the series of information security standards and guidelines developed by NIST in response to FISMA. The purpose of SP 800-39 is to provide guidance for an integrated, organization-wide program for managing information security risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation resulting from the operation and use of Federal information systems"

[indirect]

NIST SP 800-53 Rev. 4 *Security and Privacy Controls for Federal Information Systems and Organizations* [NIST 2013]

"RA-3 Risk Assessment"

Organization Response

Examples of Evidence Sought

- ❑ Copies of security RA results and corresponding improvement or mitigation actions
- ❑ Copies of recommendations and mitigation strategies provided to constituents to fix identified risks in their infrastructure
- ❑ Copies of follow-up reports showing that the problems were corrected

❑ Demonstrations or observations of configuration management, patch management, or change management systems used with the mitigation strategies or recommendations			
Scoring Criteria	Yes	No	Evidence
Required			
2.1.2.01 Control: Criteria exist for prioritizing risks based on business impact.	❒	❒	
2.1.2.02 Control: Documented guidance exists for helping constituents apply remediation strategies for the identified vulnerabilities.	❒	❒	
2.1.2.03 Control: Personnel are aware of, knowledgeable of, and consistently follow the processes and technologies for performing this task.	❒	❒	
2.1.2.04 Control: Personnel are appropriately trained on countermeasures and remediation strategies for risks.	❒	❒	
2.1.2.05 Control: Personnel are appropriately trained about the policies and processes for providing assistance to constituents.	❒	❒	
2.1.2.06 Activity: The results of the security RAs are used to determine the potential impacts of computer security incidents and identify improvements to constituent infrastructure that could prevent them.	❒	❒	
2.1.2.07 Activity: Recommendations for mitigating risks or security issues identified in RAs are provided to the constituents.	❒	❒	
Recommended Best Practices			
2.1.2.08 Control: The results of the security RA are accessible by the group(s) providing assistance in implementing risk mitigation strategies and recommendations.	❒	❒	
2.1.2.09 Activity: Technical recommendations, guidance, and support given to constituents to help with correcting the security problems and vulnerabilities that have been identified in a security RA are tracked and recorded for future use.	❒	❒	
Institutional and Quality Improvement			
2.1.2.10 Control: Documented procedures exist for helping constituents apply remediation strategies for identified vulnerabilities.	❒	❒	

2.1.2.11 Control: Personnel are aware of, knowledgeable of, and consistently follow the procedures for performing this task.	❒	❒	
2.1.2.12 Quality: A process and criteria exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	
2.1.2.13 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒
Not Applicable		❒	**Not Observed**	❒

Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement

- Train personnel for any other tasks they may need to perform as part of the remediation (e.g., vulnerability patching, security awareness training, and network defense configuration).
- Achieve greater efficiency by maintaining and updating a prioritized list of criteria for how vulnerabilities might affect the infrastructure. This list can be used to determine which vulnerabilities must be addressed first.

2.2 PREVENTION

2.2.1 The organization has an institutionalized malware prevention program.

Priority I

Clarification

This capability ensures that an institutionalized program exists for organization-wide malware prevention. This includes security awareness training for end-users, it also includes having installed AV software installed as appropriate. The malware software should have automated updates, and documented guidance for preventing malware activity.

Malware can include viruses, worms, Trojan horse programs, spyware, botnets, rootkits, and other attack vectors. Malware can be delivered through phishing, email, and malicious or compromised websites; along with other delivery methods and attack vectors.

A malware incident prevention capability includes but is not limited to

- installing and maintaining anti-malware software tools across the organization including at the perimeter, on end-user systems, and on other systems as appropriate
- ability to quarantine files or emails containing malware or suspicious content
- monitoring anti-malware sites and organizations to gather intelligence on new attack vectors and techniques
- alerting the organization to potential or current malware threats and corresponding remediation guidance
- keeping up-to-date on new developments in malware through research, training, mentoring, and other professional development efforts
- providing end user training on ways to prevent malware from being installed as part of security awareness training or system hardening

Organizational collaboration and coordination of malware prevention requires defined processes, roles, and responsibilities both internally and externally.

Team Guidance

This function might be outsourced or handled by another part of the organization. In that case, this capability should be applied to that group and its activities.

There is a separate capability related to security awareness training, refer to that capability to evaluate the effectiveness of any security training. This malware prevention capability only looks to see that there is some training for end users on preventing malware.

This capability is only addressing malware prevention. The detection of malware is covered under the normal monitoring and detection capabilities (3.1.1); the response to malware incidents is also covered under the normal response capabilities (e.g., 4.3.2).

Note that there is a separate capability under the Analysis portion of this instrument that addresses malware analysis (4.2.9). The malware prevention capability does not address malware analysis.

References

Regulatory References: None

[indirect]

FISMA Sec 3544 *Federal agency responsibilities* (b)(3) and (7) [OLRC 2003]

> "(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] to provide information security for the information and information systems that support the operations and assets of the agency […] that includes—
> (3) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate […]
> (7) procedures for detecting, reporting, and responding to security incidents […]"

Guidance References:

NIST SP 800-83 *Guide to Malware Incident Prevention and Handling* [Mell et al. 2005b]

> "Executive Summary
> [p ES-1 – ES-4]
>
> Organizations should develop and implement an approach to malware incident prevention.
> Organizations should ensure that their policies support the prevention of malware incidents.
> Organizations should incorporate malware incident prevention […] into their awareness programs.
> Organizations should have vulnerability mitigation capabilities to help prevent malware incidents.
> Organizations should have threat mitigation capabilities to assist in containing malware incidents.
> […]
> Organizations should establish malware incident prevention […] capabilities that address current and short-term future threats."

NIST SP 800-53 Rev. 4 *Security and Privacy Controls for Federal Information Systems and Organizations* [NIST 2013]

> "APPENDIX F: SECURITY CONTROL CATALOG
> SI-3 MALICIOUS CODE PROTECTION:
>
> **Control:** The organization:
>
> (a.) Employs malicious code protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code
> (b.) Updates malicious code protection mechanism whenever new releases are available in accordance with organizational configuration management policy and procedures;
> (c.) Configures malicious code protection mechanisms to: Perform periodic scans of the information system […] and real-time scans of files from external sources […] as the files are downloaded, opened, or executed in accordance with organizational security policy; and [Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator […] in response to malicious code detection; and
> (d.) Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system."

Organization Response			
Examples of Evidence Sought			
❑ Documentation of malware prevention strategy or guidance ❑ Documentation of rules for quarantining email or files containing malware. ❑ Installed AV software and configuration files ❑ Logs showing AV software updates ❑ Recent email or web malware warnings and advisories sent to constituents ❑ Recent information from vendors on malware attacks against their products and services			
Scoring Criteria	Yes	No	Evidence
Required			
2.2.1.01 Control: Personnel are appropriately trained on the process and technologies used to support the malware prevention program.	❒	❒	
2.2.1.02 Activity: Available, approved anti-malware software is used in accordance with organizational requirements.	❒	❒	
2.2.1.03 Activity: Sources of information on emerging malware (e.g., FIRST, vendor AV sites, and other similar organizations) are reviewed.	❒	❒	
2.2.1.04 Activity: Constituents are alerted to emerging or current malware threats per SLA or organizational requirements.	❒	❒	
2.2.1.05 Activity: Constituents' networks and systems are scanned continuously for malicious activity and the presence of malware.	❒	❒	
2.2.1.06 Activity: Malware program personnel can receive alerts, and download and implement any required signatures from vendor or AV sites.	❒	❒	
2.2.1.07 Activity: A current list of POCs for malware notifications and alerts is maintained.	❒	❒	
Recommended Best Practices			
2.2.1.08 Control: An enterprise-wide policy exists for establishing and maintaining a malware prevention program.	❒	❒	

2.2.1.09 Activity: Malware signatures from vendors are updated automatically according to organizational or SLA timeframes.	❒	❒	
Institutional and Quality Improvement			
2.2.1.11 Control: Documented procedures exist that describe the process and method used (including notifications, alerts, and remediation assistance) to provide this malware prevention program.	❒	❒	
2.2.1.12 Quality: Personnel are aware of, knowledgeable of, and consistently perform or use the procedures, processes, methodologies, and technologies for performing this task.	❒	❒	
2.2.1.13 Quality: A process and criteria exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	
2.2.1.14 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒
Not Applicable		❒	**Not Observed**	❒

Evidence Collected					
Document Review		Interviews		Direct Observation	
Notes					

Suggestions for Improvement

- Implement an organization-wide program for automatic updates.
- Consider using multiple audio/video (A/V) products from different vendors for more robust coverage of AV signatures.
- Institute a 24/7 malware capability.
- Monitor AV and alert websites and mailing lists daily.
- Define document types and create corresponding templates for disseminating information.
- Improve malware analysis techniques, build a test environment or lab facility, and add automated tools for collecting information on malware.
- Develop technical relationships with trusted experts (e.g., A/V equipment vendors, CERT Coordination Center [CERT/CC]).
- Keep POC lists up-to-date, reviewing them at least monthly.
- Coordinate reports on a consistent and timely basis with appropriate contacts.
- Train end-user staff to recognize various types of malware, and report malware activities in a timely fashion.
- Train end-user staff to prevent malware attacks by following best practices for secure system use.

2.3 OPERATIONAL EXERCISES FOR INCIDENT MANAGEMENT

2.3.1 Operational exercises are conducted to assess the IM function of the organization.

Priority II

Clarification

This capability requires some form of operational exercises for computer security or computer network defense to be conducted at least once a year. These exercises

- look at the adequacy of processes and procedures (through incident scenario exercises); for example, perform triage, respond to events and incidents in a timely manner, notify correct people, protect data during transmission, or meet SLAs
- may involve mock or test incident exercises implemented either online or via tabletop; penetration testing or red teaming; or other comparable exercises
- may look for technical and organizational vulnerabilities and weaknesses (through penetration testing)
- can be done across the whole organization or as requested for specific organizational business units
- may be internal to the organization or part of broader, inter-organization exercises, although broader multi-organization exercises should NOT be the only form of operational exercise conducted (The type of operational exercises that are approved and performed may be designated by the organization or determined by other relevant requirements.)

This capability includes the ability to provide support to constituents who want to either conduct their own exercises or contract the service out.

The support provided can include

- maintaining a vetted list of vendors or POCs as sources of operational exercises
- helping constituent choose or find a source for operational exercises
- actually performing, conducting, or coordinating the operational exercise

Team Guidance

This capability ensures operational exercises of some kind are conducted periodically or upon request by reliable, capable, and vetted sources.

The team should look for documented policies, procedures, and guidance for performance, support, and notification of operational exercises.

To meet this capability, organizations must perform at least one type of computer security or operational exercise for computer network defense mentioned in the Clarification section.

References

Regulatory References:

FISMA Sec 3544 *Federal agency responsibilities* (b)(5) [OLRC 2003]

"(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] to provide information security for the information and information systems that support the operations and assets of the agency […] that includes—
(5) periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually, of which such testing—
(A) shall include testing of management, operational, and technical controls of every information system identified in the inventory required under section 3505(c); and
(B) may include testing relied on in an evaluation under section 3545"

Guidance References:

NIST SP 800-53 Rev. 4 *Security and Privacy Controls for Federal Information Systems and Organizations* [NIST 2013]

"IR-3 *Incident Response Testing*
The organization tests the incident response capability for the information system [*Assignment: organization-defined frequency*] using [*Assignment: organization-defined tests*] to determine the incident response effectiveness and documents the results."

NIST SP 800-84 *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities* [Grance 2006]

"Organizations have information technology (IT) plans in place, such as contingency and computer security incident response plans, so that they can respond to and manage adverse situations involving IT. These plans should be maintained in a state of readiness, which should include having personnel trained to fulfill their roles and responsibilities within a plan, having plans exercised to validate their content, and having systems and system components tested to ensure their operability in an operational environment specified in a plan.[…]

Exercises. An exercise is a simulation of an emergency designed to validate the viability of one or more aspects of an IT plan. […]

Tabletop Exercises. Tabletop exercises are discussion-based exercises where personnel meet in a classroom setting or in breakout groups to discuss their roles during an emergency and their responses to a particular emergency situation. […]

Functional Exercises. Functional exercises allow personnel to validate their operational readiness for emergencies by performing their duties in a simulated operational environment. […]"

NIST SP 800-61 Rev. 2 *Computer Security Incident Handling Guide* [Cichonski 2012]

"Sec 2.4.3 Incident Response Personnel

Develop incident handling scenarios and have the team members discuss how they would handle them. Appendix A contains a set of scenarios and a list of questions to be used during scenario discussions."

[indirect]

"Sec 2.3.3 Procedure Elements

[p 2-4]

SOPs should be tested to validate their accuracy and usefulness […]"

Organization Response

Examples of Evidence Sought
❑ Exercise materials, scenarios, or plans ❑ Announcements of exercises ❑ Instructions on how to conduct or participate in the exercises ❑ Schedule of exercises ❑ Forms for requesting exercise assistance or support ❑ List of participants engaged in exercises previously conducted ❑ Recommendations on types and sources of exercises provided to the organization ❑ Results and lessons learned from exercises ❑ POC list with appropriate organizations and trusted agents to contact for conducting operational exercises ❑ Descriptions of the potential impact of operational exercises on organizational systems ❑ Software or tools used to conduct the exercises (e.g., penetration testing tools, virtual environments) ❑ Observation of exercises being conducted

Scoring Criteria	Yes	No	Evidence
Required			
2.3.1.01 Prerequisite: Organizational management has given approval and/or guidance for conducting operational exercises.	❒	❒	
2.3.1.02 Control: Documented policy or guidance exists that requires periodic (at least annual) operational exercises.	❒	❒	
2.3.1.03 Control: Guidance exists for performing the operational exercises.	❒	❒	
2.3.1.04 Control: Personnel are appropriately trained on the process and supporting technologies used to conduct operational exercises.	❒	❒	
2.3.1.05 Activity: Incident management personnel conduct or support operational exercises.	❒	❒	
2.3.1.06 Activity: The appropriate personnel are notified of operational exercises per guidance for this activity.	❒	❒	
2.3.1.07 Activity: The results from, impacts of, and lessons learned from conducting operational exercises are captured, recorded, and incorporated.	❒	❒	

Recommended Best Practices			
2.3.1.08 Activity: A list of types and sources of exercise providers (e.g., other departments or organizations) is maintained for operational exercises.	❒	❒	
2.3.1.09 Activity: Current incident management processes and procedures are validated during operational exercises.	❒	❒	
2.3.1.10 Activity: Incident management personnel help constituents identify the need for operational exercises, the most appropriate types of exercises, and possible operational exercise providers or materials.	❒	❒	
Institutional and Quality Improvement			
2.3.1.11 Control: Documented procedures exist that outline the roles, responsibilities, scope, appropriate tools, and notification requirements for operational exercises.	❒	❒	
2.3.1.12 Quality: Personnel are aware of, knowledgeable of, and consistently follow the procedures, processes, methodologies, and technologies for performing this task.	❒	❒	
2.3.1.13 Quality: A process and criteria exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	
2.3.1.14 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒
Not Applicable		❒	**Not Observed**	❒

Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement
• Implement a plan for quarterly testing that uses various combinations of techniques or approaches, such as penetration testing in combination with a mock exercise, and so forth.

2.4 TRAINING AND GUIDANCE

2.4.1 Guidance is provided to constituents on best practices for protecting their systems and networks.

Priority II

Clarification

This capability determines whether a defined process and methodology is in place to provide constituents with guidance on best practices for protecting systems and networks. These best practices can include methods for hardening system and network configurations, or installing defenses such as firewalls and routers. Guidance can be general or focus on specific networks and systems, and it can be given via training, presentations, mentoring, advisories, or other written technical publications.

Team Guidance

The team should look for evidence that current and appropriate guidance or best practices for securing systems and networks is provided. This guidance might not be provided by the incident management function but rather by another group (e.g., IT). If that is the case, that group should be evaluated for this capability.

References

Regulatory References:

FISMA Sec 3544 *Federal agency responsibilities* (b)(3) and (4) [OLRC 2003]

> "(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] to provide information security for the information and information systems that support the operations and assets of the agency […] that includes—
>
> (3) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate […]
>
> (4) security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of—
>
> (A) information security risks associated with their activities; and
>
> (B) their responsibilities in complying with agency policies and procedures designed to reduce these risks"

Guidance References:

NIST SP 800-61 Rev 2 *Computer Security Incident Handling Guide* [Cichonski 2012]

> "Sec 3.1.2 Preventing Incidents
>
> Although incident response teams are generally not responsible for securing resources, they can be advocates of sound security practices. Other documents already provide good advice on general security concepts and operating system and application-specific guidance." "http://csrc.nist.gov/publications/PubsSPs.html provides links to the NIST SP on computer security, which include documents on OS and application security baselines."

A Step-By-Step Approach on How to Set Up A CSIRT [ENISA, 2006]

> "A.2 CSIRT Services Security Consulting CSIRTs can be used to provide advice and guidance on the best security practices to implement for constituents' business operations. A CSIRT providing this service is involved in preparing recommendations or identifying requirements for purchasing, installing, or securing new systems, network devices, software applications, or enterprise-wide business processes. This service includes providing guidance and assistance in developing organizational or constituency security policies. It can also involve providing testimony or advice to legislative or other government bodies."

Organization Response

Examples of Evidence Sought

- ❑ Copies of recommended general and specific best practice guidance given to constituents
- ❑ Training or presentation material
- ❑ Technical publications that provide best practice guidelines
- ❑ Observation of personnel providing best practice guidance

Scoring Criteria	Yes	No	Evidence
Required			
2.4.1.01 Control: Incident management personnel are appropriately trained on the process and supporting technologies used to provide guidance on best practices.	❒	❒	
2.4.1.02 Control: Incident management personnel are appropriately trained on best practices and strategies for protecting constituents' networks and systems.	❒	❒	
2.4.1.03 Activity: Guidance is provided on best practices for protecting constituents' networks and systems.	❒	❒	
2.4.1.04 Quality: Best practice information is up to date, current, and relevant to the constituents.	❒	❒	
Recommended Best Practices			
2.4.1.05 Activity: Designated incident management personnel meet with constituents to better understand its needs and requirements.	❒	❒	
2.4.1.06 Activity: Designated incident management personnel check with constituents to see if the implemented best practices were effective.	❒	❒	

Institutional and Quality Improvement			
2.4.1.07 Control: Documented procedures exist for providing and updating general, best practice guidelines for protecting constituents' networks and systems.	❒	❒	
2.4.1.08 Quality: Personnel are aware of, knowledgeable of, and consistently follow the procedures and processes for performing this task.	❒	❒	
2.4.1.09 Quality: A process and criteria exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	
2.4.1.10 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒
Not Applicable		❒	**Not Observed**	❒

Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement
• Having access to constituents' network diagrams, configurations, and critical systems and data (if available) can help determine the most appropriate guidance to provide.

2.4 TRAINING AND GUIDANCE

2.4.2 Constituents are provided with security education, training, and awareness (ETA).

Priority I

Clarification

This capability determines whether constituents receive security education, training, and awareness (ETA) regularly and follows a documented curriculum.

This capability assesses the process and methodology by which the organization's security ETA programs are provided. This provision can take many forms, such as identifying training requirements and gaps for each constituent group, providing input for a security curriculum, or developing and delivering security ETA. Incident management personnel can help identify where organizational employees require more guidance to better conform to accepted security practices and organizational security policies.

Security awareness can be increased through courses, technical guidance, reports, posters, newsletters, websites, or other informational resources that explain security best practices and provide advice on precautions to take. Activities may also include scheduling meetings and seminars to keep constituents up to date with ongoing security procedures and potential threats to their systems. Topics covered can include

- security guidelines, such as creating good passwords, handling secure data, or avoiding identify theft
- malicious code types, propagation, and remediation techniques
- procedures for installing and using AV software, personnel firewalls, or spyware detectors
- incident reporting guidelines detailing what suspicious or malicious behavior to report, how, and to whom
- appropriate incident prevention and response methods
- other information necessary to protect, detect, report, and respond to computer security incidents

Materials should be consistent and up to date. A review and update frequency cycle should be implemented to ensure quality.

Team Guidance

If security is an outsourced capability, defining security ETA requirements and providing security training might be done by the external service provider. Or this function might be handled by another part of the organization. In both cases, this capability should be applied to the relevant group.

References

Regulatory References:

FISMA Sec 3544 *Federal agency responsibilities* (b)(4) [OLRC 2003]

"(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] to provide information security for the information and information systems that support the operations and assets of the agency […] that includes—

(4) security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of—

(A) information security risks associated with their activities; and

(B) their responsibilities in complying with agency policies and procedures designed to reduce these risks"

Guidance References:

NIST SP 800-50 *Building an Information Technology Security Awareness and Training Program* [Wilson 2003]

"This document provides guidelines for building and maintaining a comprehensive awareness and training program, as part of an organization's IT security program."

NIST SP 800-53 Rev. 4 *Security and Privacy Controls for Federal Information Systems and Organizations* [NIST 2013]

"AT-1 Security Awareness and Training Policy and Procedures
Control: The organization:

(a.) Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:

1. A security awareness and training policy […]
2. Procedures […]

(b.) Reviews and updates the current:

1. Security awareness and training policy [*Assignment: organization-defined frequency*]; and
2. Security awareness and training procedures [*Assignment: organization-defined frequency*].

AT-2 Security Awareness Training

Control: The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors) […]

AT-3 Role-Based Security Training

Control: The organization provides role-based security training to personnel with assigned security roles and responsibilities […]

AT-4 Security Training Records
Control: The organization:

a. Documents and monitors individual information system security training activities […]
b. Retains individual training records for [*Assignment: organization-defined time period*]."

NIST 800-61 Rev 2 *Computer Security Incident Handling Guide* [Cichonski 2012]

"Sec 2.5 Incident Response Team Services

Education and Awareness. Education and awareness are resource multipliers—the more the users and technical staff know about detecting, reporting, and responding to incidents, the less drain there should be on the incident response team. […]"

Expectations for Computer Security Incidents [NWG 1998]

"Sec 3.5.2. Proactive Activities

Usually additional or optional, proactive services might include…Education and training"

A Step-By-Step Approach on How to Set Up a CSIRT [ENISA, 2006]

"A.2 CSIRT Services

Awareness Building

CSIRTs may be able to identify where constituents require more information and guidance to better conform to accepted security practices and organizational security policies. Increasing the general security awareness of the constituent population not only improves their understanding of security issues but also helps them perform their day-today operations in a more secure manner. […]

Education/Training

This service involves providing information to constituents about computer security issues through seminars, workshops, courses, and tutorials. […]"

Organization Response

Examples of Evidence Sought

- ❑ ETA requirements
- ❑ ETA curricula and training plans
- ❑ Training presentations and educational materials
- ❑ Security awareness posters, articles, or publications
- ❑ Evaluations of training programs
- ❑ Training and curriculum development systems and software used to provide ETA materials
- ❑ Training and curriculum methods and equipment, including classroom instruction, computer-based training (CBT), and web presentations
- ❑ Observations of ETA delivery in person or via CBT or distance education

Scoring Criteria	Yes	No	Evidence
Required			
2.4.2.01 Control: A documented policy exists that requires constituents to receive general security awareness training and education.	❒	❒	
2.4.2.02 Control: Personnel are appropriately trained on the process and supporting technologies used to develop and provide security ETA assistance.	❒	❒	
2.4.2.03 Control: A group or person is designated as having responsibility for security and awareness training for constituents.	❒	❒	

2.4.2.04 Activity: Training requirements are gathered and documented.	❒	❒	
2.4.2.05 Activity: Security ETA is provided to constituents upon request or SLA.	❒	❒	
2.4.2.06 Activity: Periodic refresher training for security ETA is provided upon request or SLA.	❒	❒	
2.4.2.07 Quality: The ETA material and content provided are up to date and relevant.	❒	❒	
Recommended Best Practices			
2.4.2.08 Activity: If incident management personnel are not responsible for ETA, a formal method exists for them to provide input to constituent ETA curriculum and materials on security.	❒	❒	
2.4.2.09 Activity: Constituents get help identifying training requirements to strengthen any areas of weakness.	❒	❒	
2.4.2.10 Activity: More than just mandatory yearly security awareness training is provided.	❒	❒	
Institutional and Quality Improvement			
2.4.2.11 Control: Documented procedures exist that define how ETA requirements should be collected and how corresponding ETA is provided to employees.	❒	❒	
2.4.2.12 Quality: Personnel are aware of and knowledgeable about security awareness methodologies and practices.	❒	❒	
2.4.2.13 Quality: A process and criteria (such as relevance, accuracy, completeness, and usefulness) exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	
2.4.2.14 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒

Not Applicable	❒	Not Observed	❒

Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement

- Implement a formalized process for collecting ETA requirements and developing the corresponding curriculum and materials.
- Train ETA-development personnel on instructional design, and curriculum issues and methodologies.

2.5 VULNERABILITY MANAGEMENT

2.5.1 A patch management and alert program exists. **Priority I**

Clarification

This capability requires a patch management and alert program to be established within the organization. While this program does not have to be managed by incident management personnel, they should be informed about all discovered vulnerabilities and corresponding alerts, patches, fixes, and other mitigations.

A patch management and alert program should include mechanisms for

- identifying and tracking organization-impacting vulnerabilities and their corresponding fixes
- alerting constituents and other stakeholders about discovered vulnerabilities and corresponding mitigations
- providing guidance for patch installation
- monitoring patch management activities
- performing patch installation as appropriate
- providing follow-up to ensure patches are installed correctly
- helping the constituents get extensions when patching cannot be done immediately

Patches and corresponding patch guidance can be disseminated to constituents for installation, or the patches can be installed on component systems by incident management personnel or other centralized IT or patch management personnel. Whatever process is in place, there must be coordination with system and network administrators for systems that incident management personnel do not have control over. That coordination can ensure that systems to be patched by the relevant system and network administrators are indeed patched.

Whoever is responsible for the maintenance and control of the patch management and alert system should seek information about all patch notifications from as many sources as possible, including software and hardware vendors, other vulnerability analysis and reporting organizations, and other security experts. Tracking the following information in a database or tracking system can provide a history of vulnerability actions for the organization and provide a source mechanism for trend analysis:

- patch notifications
- impacts on organizational sites
- actions taken

This capability might be split across multiple actors. For example, incident management personnel may keep up-to-date with new patches and then pass that information to an IT management group who actually maintains the patch management system and servers.

Patching may not be feasible for all systems or may require significant testing. Some systems may require new system certifications if they are changed (patched). The organization needs to know which systems fall into these categories and

- ensure appropriate actions are taken to monitor those systems

- conduct testing to prevent patches from affecting operational or production systems
- ensure appropriate actions are taken to mitigate security risks if patching cannot be done

Team Guidance

The team should ensure that the capability is consistently met across all parts of the organization (i.e., any part of the organization involved in patch management activities).

The team should look for evidence that notices of new patches are received, constituents are notified of available patches, the patches are installed (incident management personnel may provide assistance), and appropriate policies, procedures, and training are documented for conducting these activities.

References

Regulatory References: None

[indirect]

FISMA 3544 *Federal agency responsibilities* (b)(3) [OLRC 2003]

> "(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] to provide information security for the information and information systems that support the operations and assets of the agency […] that includes—
>
> (3) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate […]"

Guidance References:

NIST SP 800-40 Ver. 2. *Creating a Patch and Vulnerability Management Program* [Mell 2005a]

> "This publication is designed to assist organizations in implementing security patch and vulnerability remediation programs. It focuses on how to create an organizational process and test the effectiveness of the process. It also seeks to inform the reader about the technical solutions that are available for vulnerability remediation."

NIST SP 800-53 Rev. 4 *Security and Privacy Controls for Federal Information Systems and Organizations* [NIST 2013]

> "SI-2 Flaw Remediation
>
> Control: The organization:
>
> (a.) Identifies, reports, and corrects information system flaws;
> (b.) Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation;
> (c.) Installs security-relevant software and firmware updates within [*Assignment: organization-defined time period*] of the release of the updates; and
> (d.) Incorporates flaw remediation into the organizational configuration management process."

NIST SP 800-61 Rev 2 *Computer Security Incident Handling Guide* [Cichonski 2012]

> "Sec 2.5 Incident Response Team Services
>
> Advisory Distribution.
>
> A team may issue advisories within the organization regarding new vulnerabilities and threats. Automated methods should be used whenever appropriate to disseminate information; for example, the National Vulnerability Database (NVD) provides information via XML and

RDF Site Summary (RSS) feeds when new vulnerabilities are added to it. Advisories are often most necessary when new threats are emerging, such as a high-profile social or political event (e.g., celebrity wedding) that attackers are likely to leverage in their social engineering. Only one group within the organization should distribute computer security advisories to avoid duplicated effort and conflicting information."

Organization Response

Examples of Evidence Sought

- ❑ Demonstrations of automated tools for distributing and installing patches on constituents' systems
- ❑ Copies of patch alerts and notifications sent to constituents
- ❑ Mail from vendors or others announcing patch availability
- ❑ Copies of extension or exemption requests made
- ❑ Records of patches that have been installed
- ❑ List of websites visited to acquire patch and mitigation updates
- ❑ Lists of systems that cannot be patched and alternative mitigations taken

Scoring Criteria	Yes	No	Evidence
Required			
2.5.1.01 Control: Designated responsibilities exist for patch management.	❒	❒	
2.5.1.02 Control: A current inventory exists of the systems and applications that are partially patched or cannot be patched due to business, compliance, or other reasons.	❒	❒	
2.5.1.03 Control: Personnel are trained appropriately on the processes and supporting technologies used for patch management activities.	❒	❒	
2.5.1.04 Control: A current list is maintained of constituent POCs, with primaries and alternates to contact about alerts and patches.	❒	❒	
2.5.1.05 Activity: Patch management personnel receive vendor and other security group patch notifications, including technical advisories.	❒	❒	
2.5.1.06 Activity: Patch management personnel research numerous sources of vulnerability and corresponding patch information.	❒	❒	

2.5.1.07 Activity: Vulnerability and patch information is analyzed to determine if the information is relevant to the organization.	❒	❒	
2.5.1.08 Activity: Patch notifications and vulnerability alerts and advisories are developed and disseminated based on organization requirements.	❒	❒	
2.5.1.09 Activity: Patches are tested and verified before installation.	❒	❒	
2.5.1.10 Activity: Constituents' systems are patched according to organizational guidance. (Patches can be distributed to constituents for installation or installed directly on their systems.)	❒	❒	
2.5.1.11 Activity: Patch implementation by constituents is monitored, and technical assistance is provided as required.	❒	❒	
2.5.1.12 Activity: System vulnerabilities that cannot be patched are mitigated in an alternative way that meets organizational guidance.	❒	❒	
2.5.1.13 Activity: Processes are in place to monitor systems that cannot be patched.	❒	❒	
2.5.1.14 Quality: The patch information provided to constituents is up to date.	❒	❒	
Recommended Best Practices			
2.5.1.15 Control: A process exists for testing and verifying patches before installation.	❒	❒	
2.5.1.16 Control: A process exists for disseminating patches and patch information.	❒	❒	
2.5.1.17 Control: A process exists for monitoring patch implementation by the organization.	❒	❒	
2.5.1.18 Control: A process exists for submitting and handling extension requests for the organization.	❒	❒	
2.5.1.19 Control: A process exists for determining and implementing the actions needed to isolate or control risk to an unpatched system.	❒	❒	

2.5.1.20 Activity: Network and system monitoring is coordinated with other responsible parties for systems not under the direct control of incident management personnel.	❒	❒	
2.5.1.21 Activity: The constituents receive help with extension requests, particularly with describing technical risks associated with noncompliance.	❒	❒	
2.5.1.22 Activity: A searchable archive exists where patch notifications (alerts, bulletins, and advisories) are stored securely.	❒	❒	
2.5.1.23 Quality: Patch management personnel review the constituent patch management procedures to determine if they are sufficient.	❒	❒	
Institutional and Quality Improvement			
2.5.1.24 Control: Documented procedures exist for patch management activities.	❒	❒	
2.5.1.25 Quality: Personnel are aware of, knowledgeable of, and consistently follow the procedures.	❒	❒	
2.5.1.26 Quality: A process and criteria exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	
2.5.1.27 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒	
Not Applicable		❒	**Not Observed**	❒	

Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes
Suggestions for Improvement
None

2.5 VULNERABILITY MANAGEMENT

2.5.2 Proactive vulnerability assessment is performed on constituent networks and systems.

Priority I

Clarification

This capability focuses on whether a regularly performed activity and a supporting defined process exist for assessing vulnerabilities on the constituents' infrastructure. Having both ensures that vulnerabilities are identified and addressed in a timely manner to prevent or minimize damage to the organization. The goal is to ensure that vulnerabilities are identified and remediated faster than they can be exploited. A central part of vulnerability assessment is continually performing VS. Once vulnerabilities have been identified, the constituency can prioritize remediation activities.

This activity can be performed by a CSIRT or by another part of the organization's incident management function. It can also be done by other divisions or branches within the organization. VS tools should be kept up-to-date with the latest known vulnerabilities (e.g., through Common Vulnerabilities and Exposures/National Vulnerability Database [CVE/NVD]). Whoever performs VS should be able to determine the relevance of a vulnerability to the organization's networks and systems. A comparison of VS results with event logs should be performed to determine if the vulnerabilities were exploited.

If VS is performed by other divisions or branches in the organization, incident management personnel may only perform tasks that involve providing information on implementing VS methodologies and tools to them. Best practices recommend that the output of any VS done by those divisions or branches should be fed back to the CSIRT or incident management personnel. VS of the network perimeter will make the organization aware of weaknesses that can be identified by external actors.

Constituents should be encouraged to proactively look for threats to their infrastructure to protect it from known attacks and vulnerabilities. This approach allows problem areas to be mitigated in a proactive manner, increasing the overall security of the organization.

If VS is performed by the CSIRT or incident management personnel, processes and forms should be in place so that constituents can request scanning on a periodic or regular basis. Agreement with the organization on what the results report contains should also be outlined.

If the constituents perform the VS activities themselves instead of incident management personnel, agreement on what information should be shared or fed back to the incident management function could be discussed and agreed to as a best practice. This information can be used by incident management personnel for analysis and trending.

Team Guidance

If business units instead of incident management personnel perform this function, the assessment team should ensure that information is sent back to the incident management function and that the personnel in the function are aware of what type and frequency of scans are being done. If this capability is performed by another group or outsourced, the assessment team should assess that other group or entity.

References

Regulatory References:

FISMA Sec 3544 *Federal agency responsibilities* (b)(5) [OLRC 2003]

> "(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] to provide information security for the information and information systems that support the operations and assets of the agency […] that includes— […]
>
> (5) periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually, of which such testing—
>
> (A) shall include testing of management, operational, and technical controls of every information system identified in the inventory required under section 3505(c); and
>
> (B) may include testing relied on in an evaluation under section 3545"

Guidance References:

NIST SP 800-53 Rev. 4 *Security and Privacy Controls for Federal Information Systems and Organizations* [NIST 2013]

> "[F-94] RA-5 *Vulnerability Scanning*
>
> Control: The organization:
>
> a) Scans for vulnerabilities in the information system and hosted applications [*Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process*] and when new vulnerabilities potentially affecting the system/applications are identified and reported;
> b) *Employs* vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
>
> 1. Enumerating platforms, software flaws, and improper configurations;
> 2. Formatting checklists and test procedures; and
> 3. Measuring vulnerability impact;
>
> c) *Analyzes* vulnerability scan reports and results from security control assessments"

By-Step Approach on How to Set Up A CSIRT [ENISA, 2006]

> "A.2 CSIRT Services
>
> Vulnerability analysis
>
> The CSIRT performs technical analysis and examination of vulnerabilities in hardware or software. This includes the verification of suspected vulnerabilities and the technical examination of the hardware or software vulnerability to determine where it is located and how it can be exploited. […]"

Organization Response

Examples of Evidence Sought

- ❑ Authorization to install tools and perform scans

- ❑ Examples of constituent request forms or written requests for assistance
- ❑ Copies of VS results and analysis
- ❑ Demonstration or observation of VS tools and methodologies
- ❑ Review or observation of vulnerability tracking and reporting tools and methodologies

Scoring Criteria	Yes	No	Evidence
Required			
2.5.2.01 Control: Written permission from management (or other documentation) exists to use VS tools on the constituents' systems and networks.	❒	❒	
2.5.2.02 Control: Documented policies exist requiring periodic or regular VS of constituents' networks and systems (at least once a year).	❒	❒	
2.5.2.03 Control: Personnel are appropriately trained on the process, methods, and supporting technologies used to conduct VS, and perform corresponding analysis and reporting.	❒	❒	
2.5.2.04 Activity: Proactive vulnerability scans are run on constituents' networks and systems.	❒	❒	
2.5.2.05 Activity: VS tools are regularly updated to address new vulnerabilities.	❒	❒	
2.5.2.06 Activity: VS tools are tested and evaluated prior to their use on constituents' networks and systems.	❒	❒	
2.5.2.07 Activity: VS results are analyzed, recorded, and tracked.	❒	❒	
2.5.2.08 Activity: Analysis includes a determination of what information about the systems and networks is discoverable by adversaries.	❒	❒	
2.5.2.09 Activity: Constituents are alerted to vulnerabilities found in their systems.	❒	❒	
2.5.2.10 Activity: Lessons learned from vulnerability assessments are incorporated into vulnerability assessment processes, training, and testing.	❒	❒	

Recommended Best Practices			
2.5.2.11 Control: Existing documentation describes the VS tools and their potential impact on constituents' networks and systems.	❒	❒	
2.5.2.12 Activity: If VS is performed by constituents, the results are forwarded to incident management personnel for further analysis or trending.	❒	❒	
2.5.2.13 Control: If VS is performed by incident management personnel, a method for business units to request a scan is documented and followed.	❒	❒	
2.5.2.14 Activity: Vulnerability scanning occurs on a continuous basis.	❒	❒	
2.5.2.15 Activity: Analyses are archived in a secure and protected manner.	❒	❒	
2.5.2.16 Activity: VS results are compared with event logs to determine if vulnerabilities were exploited.	❒	❒	
Institutional and Quality Improvement			
2.5.2.17 Control: Documented procedures exist that describe the process and method used to • obtain permission for VS on organizational systems • perform VS • analyze data gathered from VS	❒	❒	
2.5.2.18 Quality: Personnel are aware of, knowledgeable of, and consistently follow the procedures, processes, methodologies, and technologies for performing this task.	❒	❒	
2.5.2.19 Quality: A process and criteria exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	
2.5.2.20 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒

Not Applicable	❒	Not Observed	❒

Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement

- Run QA checks on the information provided to ensure it is complete, timely, accurate, clear, understandable, up-to-date, and useful, and it meets any organizational, institutional, and legal compliance guidelines.
- Train personnel on VS methodologies and tools. Having that knowledge can help those providing this assistance to ensure that all relevant systems and networks are reviewed, therefore ensuring the requestor gets useful information.
- Use automated tools to perform vulnerability scanning and tracking, and to create a vulnerability database that tracks vulnerabilities by organizational unit and tracks vulnerability remediation.
- Implement mechanisms, such as templates or web forms that constituents can use to request scanning or other assistance that can be given via written or verbal recommendations, meetings, training sessions, or VS.

2.5 VULNERABILITY MANAGEMENT

2.5.3 Constituents receive help to correct problems identified by vulnerability assessment activities.

Priority II

Clarification

This capability focuses on the provision of technical recommendations, guidance, and support to constituents to help with correcting security problems and vulnerabilities that were identified via proactive vulnerability assessment. Being able to provide such guidance requires knowledge of the criticality of the affected networks and systems as well as being able to determine the impact of exploited vulnerabilities. Depending on the level and set of incident management services provided, that help could either

- take the form of hands-on configuration, in which incident management personnel make the corrections or work with the appropriate system and network owner to make the changes
- simply be the provision of technical remediation strategies and advice

Team Guidance

This capability is applicable regardless of whether incident management personnel or organizational personnel perform the vulnerability assessments.

It is possible that incident management personnel still provide the assistance in correcting problems, even if they are not the ones doing the scanning.

If other organizational personnel provide the assistance, that group should be assessed for this capability.

References

Regulatory References:

FISMA Sec 3544 *Federal agency responsibilities* (b)(6) [OLRC 2003]

> "(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] that includes— […]
> (6) a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency"

OMB Cir A-130 *Memorandum for Heads of Executive Departments and Agencies* App III Sec A.5.a.

> "Correction of Deficiencies. Agencies shall correct deficiencies which are identified through the reviews of security for systems and major applications described above."

Guidance References:

NIST SP 800-53 Rev. 4 *Security and Privacy Controls for Federal Information Systems and Organizations* [NIST 2013]

> "[F-94] RA-5 Vulnerability Scanning
>
> The organization: […]

d. Remediates legitimate vulnerabilities [*Assignment: organization-defined response times*] in accordance with an organizational assessment of risk; and

e. Shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies)."

A Step-by-Step Approach on How to Set Up a CSIRT [ENISA, 2006]

"Vulnerability response

This service involves determining the appropriate response to mitigate or repair vulnerability. This may involve developing or researching patches, fixes, and workarounds. It also involves notifying others of the mitigation strategy, possibly by creating and distributing advisories or alerts.

Vulnerability response coordination

The CSIRT notifies the various parts of the enterprise or constituency about the vulnerability and shares information about how to fix or mitigate the vulnerability. The CSIRT verifies that the vulnerability response strategy has been successfully implemented."

Organization Response

Examples of Evidence Sought

- ❑ Copies of recommendations and remediation strategies provided to constituents for fixing identified vulnerabilities in their infrastructure
- ❑ Copies of follow-up reports showing that the problems were corrected
- ❑ Observation or demonstration of vulnerability tracking and handling mechanisms or systems showing remediation and assistance being given to constituents

Scoring Criteria	Yes	No	Evidence
Required			
2.5.3.01 Control: Personnel are appropriately trained in how to provide assistance to constituents.	❒	❒	
2.5.3.02 Control: Personnel are appropriately trained in countermeasures and remediation strategies for vulnerabilities.	❒	❒	
2.5.3.03 Activity: Recommendations are provided for correcting problems such as the vulnerabilities or security issues identified in vulnerability scanning results.	❒	❒	
2.5.3.04 Activity: The identified vulnerabilities are remediated.	❒	❒	

Recommended Best Practices			
2.5.3.05 Control: Vulnerability assessment results are available to whomever provides the assistance to the organization.	❒	❒	
2.5.3.06 Control: Criteria exist for prioritizing vulnerabilities based on business impacts.	❒	❒	
2.5.3.07 Activity: Follow-up actions are performed to ensure problems are corrected and actions are closed.	❒	❒	
Institutional and Quality Improvement			
2.5.3.08 Control: Documented procedures exist for • analyzing vulnerabilities identified in scanning • determining impacts to constituents' systems • providing assistance to constituents to address and mitigate identified vulnerabilities • documenting and archiving actions taken to assist constituents	❒	❒	
2.5.3.09 Control: Personnel are aware of, knowledgeable of, and consistently follow the procedure, processes, and technologies for performing this task.	❒	❒	
2.5.3.10 Quality: A process and criteria exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	
2.5.3.11 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒
Not Applicable		❒	**Not Observed**	❒

Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement

- Provide sufficient skills or training for incident management personnel for any other tasks that they may need to perform, such as vulnerability patching or network defense configuration.
- Maintain and update a prioritized list of criteria for how vulnerabilities might affect the infrastructure.
- Use this list to determine which vulnerabilities must be addressed first.
- Use criteria such as completeness, timeliness, accuracy, clarity, usefulness, and adherence to security best practices, institutional regulations, or legal rules and laws to evaluate the quality of performance and artifacts associated with this activity.
- Use automated tools such as patch or configuration management systems.
- Track and record all changes, and follow the organization's change management processes.

DETECT: SECTION 3 OF INCIDENT MANAGEMENT CAPABILITIES

In Detect, information about potential incidents, vulnerabilities, and other computer security or incident management information is gathered both proactively and reactively. In reactive detection, information is received from internal or external sources in the form of reports or notifications, as shown in the following examples:

- Those using the organization's computing resources may notice unusual or malicious activity and report it to the appropriate contact. Reporting may involve submitting an incident reporting form or calling the appropriate POC, such as a helpdesk or a CSIRT hotline.
- Other computer security experts may send an alert or notification that must be assessed to see if there is a potential threat to the receiver's infrastructure. For example, an external team might receive reports of a new worm propagating in its area, create an advisory or alert, and send it to a subscriber mailing list. The organization's incident management personnel see this advisory or alert, evaluate whether it might have a similar effect in their organization, and then take action based on their analysis.
- An external team might send a report to an organization alerting personnel to activity appearing to originate from within the organization. The organization then needs to review or evaluate its own systems to determine if there is a problem.

Proactive detection requires actions by the designated staff to identify suspicious activity. Personnel monitor a variety of data (e.g., host logs, firewall logs, netflows) and use intrusion detection and prevention software to monitor network behavior, looking for indications of suspicious activity. The data are analyzed, and any unusual or suspicious event information is "triaged" to the appropriate individuals for handling.

Personnel performing proactive detect capabilities may be located in various parts of an organization such as an IT group, telecommunications group, security group, or formal CSIRT. In some organizations, the IT or network operations staff perform this capability and pass on any suspicious activity, or relevant incident or vulnerability information to an established CSIRT. In such cases, it is important to have established procedures for passing on this information. Personnel performing the monitoring must have criteria to help them determine what type of alerts or suspicious activity should be escalated. Personnel who conduct proactive monitoring can include

- IT staff (e.g., network information center [NIC] staff, network operations center [NOC] staff, SOC staff, system and network administrators)
- selected members of the CSIRT staff
- third parties (e.g., MSSPs, collaborators, ISPs, trusted subject matter experts)
- coordination center staff

Proactive detection also includes technology watch or public monitoring capabilities to evaluate current information about security topics that may affect the organization's computing infrastructure. Personnel review security resources to obtain information about

- new vulnerabilities
- new attack types and threats

- new recommendations and solutions for preventing incidents
- general political, social, or sector-related information that may have relevance to ongoing or potential malicious activity

Security resources would include, for example, security mailing lists, websites, articles, or news reports that are available publicly, or aggregated information from a commercial service.

The subcategories and capabilities in the Detect category are

3.1. Network and Systems Security Monitoring—Network monitoring is an important proactive capability that allows an organization to detect suspicious activity across the enterprise. Such monitoring can provide early warnings about malicious threats or activity in the organization's infrastructures, allowing response actions to be initiated in a timely manner, containing the damage and impact that could have been done. Technologies involved in network monitoring and analysis can include IDS, IPS, anomaly detection systems (ADS), antivirus detection systems, netflow analysis tools, and network forensics analysis tools (NFAT). Incident management personnel might assist organizations with monitoring tool selection, configuration, and installation, and analysis of output for detection of possible intrusions.

3.1.1. Security monitoring is continuously performed on all constituent networks and systems.

3.2. External Sources of Incident Information—The incident management function needs to be able to receive reports of events and incidents affecting the constituents' systems that external sources detect or identify. This communication from outside could be an external group such as another CSIRT or a coordination center or even an individual with critical information.

3.2.1. Events and incidents are reported from outside the organization.

3.3. Threat and Situational Awareness—Organizations must understand the context within which network events and incidents occur. To do this they must keep up-to-date with new attack types, remediation strategies, detection strategies, best practice protection strategies, and security detection and response tools. However, to get a complete picture of the relationship of network and system traffic to current events, other political, social, economic, and financial activities must also be reviewed. This type of proactive monitoring of new and current developments is often called technology watch, public monitoring, and situational awareness. Such monitoring provides an overview of internet activity in the context of domestic and foreign developments. It can show connections between activity and attacks at different sites and help analysts better understand the scope and impact of malicious computer events and incidents.

3.3.1. Public monitoring of external security websites and other trusted sources of information is conducted.

3.3.2. Trend analysis is supported and conducted.

3.3.3. Network and system configurations or rule sets are reviewed and updated in response to changes in the threat environment, and constituents are notified of the updates.

3.3.4. Penetration testing is conducted on organizational networks and systems.

3.1 NETWORK AND SYSTEMS SECURITY MONITORING

3.1.1 Security monitoring is continuously performed on all constituent networks and systems.

Priority I

Clarification

Security monitoring is an important function that allows an organization to detect suspicious activity across its enterprise. Suspicious activity also includes unauthorized, security-relevant changes to constituent systems and networks. This capability ensures the organization can

- monitor constituent networks and systems
- analyze or monitor output to detect possible intrusions
- notify constituents of suspicious behavior
- provide guidance and recommendations on tool selection, installation, and configuration; analysis and monitoring techniques and methodologies; and network monitoring strategies
- help or train constituents to monitor their own systems

Technologies involved in security monitoring and analysis can include IDSs, IPSs, ADSs, AVSs, netflow analysis tools, NFAT, host-based monitoring, and other similar tools.

Team Guidance

The group that performs this function is the one that should be assessed relative to this function. In cases where an organization outsources monitoring completely to a third-party MSSP and includes that provider in the assessment, the capability should be applied to the MSSP. In all situations, incident management personnel need an interface to whomever performs the monitoring so the organization is notified about suspicious activity.

If an external party performs detection activities, incident management personnel or another organizational group must be engaged sufficiently and maintain a useful enough interface to have an accurate view of the organization's security posture as it relates to detection. If an established CSIRT exists, it should be able to obtain this information through a defined interface.

References

Regulatory References: None

[indirect]

FISMA Sec 3544 *Federal agency responsibilities* (b)(7) [OLRC 2003]

> "(b) AGENCY PROGRAM - Each agency shall develop, document, and implement an agency-wide information security program […] that includes […]
>
> (7) procedures for detecting […] security incidents […]"

Guidance References:

NIST SP 800-94 *Guide to Intrusion Detection and Prevention Systems* (IDPS) [Scarfone 2007]

"This publication seeks to assist organizations in understanding intrusion detection system (IDS) and IPS technologies and in designing, implementing, configuring, securing, monitoring, and maintaining intrusion detection and prevention systems (IDPS).

4. NIST SP 800-61 Rev 2 *Computer Security Incident Handling Guide* [Cichonski 2012]

5. Sec 2.5 Incident Response Team Services [intrusion detection responsibility should be assigned to another team]
   Intrusion Detection. "The first tier of an incident response team often assumes responsibility for intrusion detection. […]

Sec 3.2.2 Signs of an Incident, and Sec 3.2.3 Sources of Precursors and Indications"

NIST SP 800-137 *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* [Dempsey 2010]

"Continuous Monitoring

6. The purpose of this guideline is to assist organizations in the development of an ISCM strategy and the implementation of an ISCM program that provides awareness of threats and vulnerabilities, visibility into organizational assets, and the effectiveness of deployed security controls. […]"

NIST SP 800-53 Rev 3 *Recommended Security Controls for Federal Information Systems and Organizations* [NIST 2009a]

"CA-7 CONTINUOUS MONITORING

Control: The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes:

a. A configuration management process […]
b. A determination of the security impact […]
c. Ongoing security control assessments […]
d. Reporting the security state of the information system […]

SI-4 INFORMATION SYSTEM MONITORING

Control: The organization:

1. Monitors events […];
2. Identifies unauthorized use of the information system;
3. Deploys monitoring devices […];
4. Heightens the level of information system monitoring activity […]; and
5. Obtains legal opinion […]"

NIST Interagency Report 7756 Draft *CAESARS Framework Extension: An Enterprise Continuous Monitoring Technical Reference Architecture* [Mell 2012]

"The end goal of CAESARS FE is to enable enterprise CM by presenting a technical reference architecture that allows organizations to aggregate collected data from across a diverse set of security tools, analyze that data, perform scoring, enable user queries, and provide overall situational awareness."

DHS Continuous Asset Evaluation, Situational Awareness, and Risk Scoring Reference Architecture Report (CAESARS) [DHS 2010]

"The objective of this document is to describe a reference architecture that is an abstraction of a security posture monitoring and risk scoring system, informed by the sources noted above, and that can be applied to other agencies seeking to apply risk scoring principles to their information security program."

Organization Response

Examples of Evidence Sought
❑ Samples of logs, alerts, and reports generated by security monitoring tools ❑ Network diagrams showing placement of monitoring tools on constituent networks ❑ IDS, IPS, ADS, or AVS configuration files that specify what anomalous events trigger an alarm ❑ Documentation of actions for responding to alerts and reports generated by security monitoring tools ❑ Observations of actual monitoring activities including devices, software, and/or outputs

Scoring Criteria	Yes	No	Evidence
Required			
3.1.1.01 Control: Documented policies or guidance exist that define how constituent networks should be monitored and analyzed.	❒	❒	
3.1.1.02 Control: A strategy exists to ensure continuous network security monitoring of constituent networks and systems.	❒	❒	
3.1.1.03 Control: Criteria exist for characterizing anomalous events, including suspicious ports, protocols, and services (both network based and host based).	❒	❒	
3.1.1.04 Activity: Personnel are appropriately trained on the processes and supporting technologies used to provide security monitoring and analysis, including log file analysis.	❒	❒	
3.1.1.05 Activity: Security monitoring is conducted on all organizational networks and systems.	❒	❒	
3.1.1.06 Activity: Log analysis and correlation tools are used.	❒	❒	
3.1.1.07 Activity: Anomalous network events are characterized in support of security monitoring and intrusion detection.	❒	❒	
3.1.1.08 Activity: The analysis results of monitoring activities are disseminated to other organizational business units as specified by organizational policy or guidance.	❒	❒	

6.5.1.09 Activity: Network and system configurations or rule sets are reviewed and updated in response to changes in the threat environment and constituents are notified of the updates.	❒	❒	
Recommended Best Practices			
3.1.1.10 Control: Documented policies exist that define how various types of monitoring techniques are implemented, including heuristic and anomalous scanning.	❒	❒	
3.1.1.11 Control: Notification capabilities exist, including appropriate communications mechanisms.	❒	❒	
3.1.1.12 Control: An MOU exists that describes security monitoring responsibilities of third-party providers of organizational networks and systems.	❒	❒	
3.1.1.13 Activity: A variety of network monitoring methodologies are used based on organizational guidance including behavior-based IDS, AVS, and so forth.	❒	❒	
3.1.1.14 Activity: Host-based monitoring tools are used.	❒	❒	
3.1.1.15 Activity: Logs and other monitoring data are reviewed on a real-time basis or several times a day to detect possible intruders.	❒	❒	
3.1.1.16 Activity: Reports, alerts, and notifications are forwarded to other organizations as appropriate.	❒	❒	
3.1.1.17 Activity: There is spare equipment for any network or host monitoring tools to provide backup and recovery capabilities.	❒	❒	
3.1.1.18 Quality: Monitoring tools have automated alert capability.	❒	❒	
Institutional and Quality Improvement			
3.1.1.19 Control: Documented procedures exist defining how • to review IDS logs, including a requirement for near-real-time review • to request audit logs from organizations • organizational networks and systems should be monitored and analyzed • heuristic scanning is performed (as well as when) by IDSs, AVSs, and other network scanning tools	❒	❒	

3.1.1.20 Control: Criteria exist that define near-real-time (e.g., for review of logs).	❒	❒	
3.1.1.21 Quality: Personnel are aware and knowledgeable of network monitoring tools and techniques, including how to review logs after a potential incident is detected, and consistently follow the procedures for performing this task.	❒	❒	
3.1.1.22 Quality: Organizations are aware and knowledgeable of security monitoring activities.	❒	❒	
3.1.1.23 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒
Not Applicable		❒	**Not Observed**	❒

Evidence Collected

Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement

- Use automated tools.
- Ensure automated alerts are enabled.
- Implement multiple types of security monitoring systems.
- Ensure results are analyzed in near-real-time.
- Ensure network diagrams of monitoring system placement are available and up to date.
- Provide training to personnel on the various tools and methodologies being used.
- Study alert patterns, and build a model for typical network behavior.

3.2 EXTERNAL SOURCES OF INCIDENT INFORMATION

3.2.1 Events and incidents are reported from outside the organization. **Priority I**

Clarification

This capability focuses on the communication from outside the organization to the incident management personnel responsible for receiving reports of events and incidents (e.g., an external group such as another CSIRT, coordination centers such as US-CERT, or an individual who has information on an incident that may also be impacting the organization). For this activity to occur efficiently, defined, easy-to-use mechanisms and contact information for reporting events and incidents should exist, as appropriate. Such mechanisms facilitate the transfer of appropriate and useful information.

Team Guidance

This capability may not always be applicable because some organizations may not receive externally reported events and incidents. If it is applicable, the team should look for evidence that incidents or incident information are being reported from external sources. The team should determine that external groups or individuals can readily locate reporting POCs and mechanisms in order to make such a report and that there is some guidance on proper reporting. The team should also look for evidence that the information reported is done according to the level of security required and is properly stored and handled.

References

Regulatory References:

FISMA Sec 3544 *Federal agency responsibilities* (b)(7) [OLRC 2003]

> "(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] that includes— […]
> (7) procedures for detecting, reporting, and responding to security incidents […]"

Guidance References: None

Agency Response

Examples of Evidence Sought

- ❑ Copies of reports received from external individuals or groups
- ❑ Forms/mechanisms used to report events/incidents, with instructions and examples (e.g., email, web forms/instructions)
- ❑ Documented and up-to-date organizational POC information with appropriate contact information and alternates in an accessible place

Scoring Criteria	Yes	No	Evidence
Required			
3.2.1.01 Control: A policy or guidance exists that defines what to do with externally reported events/incidents.	❒	❒	
3.2.1.02 Control: Guidance and contact information are readily available on how external individuals or groups should report events and incidents.	❒	❒	
3.2.1.03 Activity: Incident management personnel follow the guidance for externally reported events and incidents if those reports are received.	❒	❒	
Recommended Best Practices			
3.2.1.04 Activity: Regular review of external reporting guidelines is performed, and guidelines are updated as needed.	❒	❒	
Institutional and Quality Improvement			
3.2.1.05 Control: Documented procedures exist for handling externally reported events and incidents.	❒	❒	
3.2.1.06 Quality: Personnel are aware of, knowledgeable of, and consistently follow the procedures for this activity.	❒	❒	
3.2.1.07 Quality: A process and criteria exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	
3.2.1.08 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒
Not Applicable		❒	**Not Observed**	❒

Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes
Suggestions for Improvement
None

3.3 THREAT AND SITUATIONAL AWARENESS

3.3.1 Public monitoring of external security websites and other trusted sources of information is conducted.

Priority I

Clarification

This capability focuses on whether the organization monitors security-related and general news sites in a structured manner to identify information that can be used to alert the organization to potential threats and problems. Monitoring can provide early warnings about malicious threats or activity that may have an impact on the infrastructure. Monitoring can provide a better understanding of the significance, scope, and context of an event or incident, allowing response actions to be initiated in a timely manner to contain the potential damage and impact. This approach improves the organization's overall network defense posture and allows the organization to have an agile response. Such information might be used

- in daily briefings or shift-change logs
- as rationale for IDS signature updates or changes in network monitoring configurations
- as correlation information during incident or vulnerability analysis
- as an impetus for new training for incident management and organizational personnel
- as a driver of new incident management research projects
- as information-sharing content sent to incident management staff

Part of this activity is the observation of new technical developments, new intruder activities, and related trends to help identify future threats. Topics reviewed can include legal and legislative rulings, social or political threats, and emerging technologies. Incident management personnel should extract information relevant to the security of the organization's systems and networks from sources that include security mailing lists and websites, and current news and journal articles in the fields of science, technology, politics, and government. In addition, they can communicate with other parties who are authorities in these fields to ensure they get the most accurate information or interpretation.

Team Guidance

The team should look for evidence of regular monitoring of a variety of security, news, and other trusted sites for information related to computing technologies, attacks, and threats, and for socio-political, economic, or legal information related to malicious computer security events and incidents. Policies and procedures should identify the appropriate guidelines and rules for accessing and monitoring these sites, along with methods for extracting, synthesizing, and disseminating information.

References

Regulatory References: None

Guidance References:

Good Practice Guide for Incident Management, [ENISA 2010]

"8-Incident Handling Process

8.1 Incident Report

Good Practice: Monitor forums and news websites for possible incident reports or threats. A constituent is not always aware that he is experiencing a security incident, but they might suffer downtime or slow service, which is then noticed by the press or results in questions or discussions in forums."

Organization Response

Examples of Evidence Sought

- ❑ List of criteria for what to monitor
- ❑ Records of gathered information
- ❑ Addresses or lists of websites monitored, including Security, "black-hat," news, and legal websites and archives
- ❑ Archives of emails from mailing list subscriptions
- ❑ Reports synthesized from the information gathered
- ❑ Mechanisms or methods used to monitor, synthesize, and disseminate information
- ❑ Email systems and mailing lists
- ❑ Demonstrations of research and monitoring of identified websites

Scoring Criteria	Yes	No	Evidence
Required			
3.3.1.01 Control: Trusted external sources of information have been identified.	❒	❒	
3.3.1.02 Control: A process exists that specifies how information is to be reviewed, collected, synthesized, disseminated, and used.	❒	❒	
3.3.1.03 Control: Documented safeguards and instructions exist for searching high-risk websites, such as "black-hat" sites, in a safe, non-attributable or non-traceable fashion.	❒	❒	
3.3.1.04 Control: Personnel are appropriately trained in the processes, checklists, reliable websites, and supporting technologies used to perform information-gathering or public monitoring.	❒	❒	
3.3.1.05 Control: Personnel are appropriately trained in synthesizing information in a secure, safe manner.	❒	❒	

3.3.1.06 Activity: Personnel check a variety of trusted sources of information on a daily or weekly basis.	❒	❒	
3.3.1.07 Activity: Personnel extract and synthesize information gathered.	❒	❒	
3.3.1.08 Activity: Personnel communicate notable, public monitoring information to the appropriate technical and management staff and where appropriate, to the organization.	❒	❒	
3.3.1.09 Activity: Oversight of this activity is conducted to ensure it occurs.	❒	❒	
Recommended Best Practices			
3.3.1.10 Control: One or more personnel are assigned to perform this activity on a routine basis.	❒	❒	
3.3.1.11 Control: A documented checklist exists that catalogs which sites to visit and critical information to examine each day.	❒	❒	
3.3.1.12 Activity: Monitoring activities are automated, or sources of information are automatically aggregated.	❒	❒	
3.3.1.13 Activity: Information captured or collected through monitoring activities is archived in a searchable form (i.e., database or knowledge management system).	❒	❒	
Institutional and Quality Improvement			
3.3.1.14 Control: Documented procedures exist that detail how information is to be reviewed, collected, synthesized, disseminated, and used.	❒	❒	
3.3.1.15 Quality: Personnel are aware of, knowledgeable of, and consistently follow the procedures and processes for performing this task.	❒	❒	
3.3.1.16 Quality: A process and criteria exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	
3.3.1.17 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒	
Not Applicable		❒	**Not Observed**	❒	

Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement
• Use automated tools or intelligence agents to scan for specific types of information.

3.3 THREAT AND SITUATIONAL AWARENESS

3.3.2 Trend analysis is supported and conducted. Priority II

Clarification

This capability focuses on whether the organization takes a proactive, broad-based, big-picture view of the system and network incident and vulnerability information it is collecting. Having such a view helps the organization determine trends in the types of attacks targeting it or changes in the types of malicious activity seen on its infrastructure. This analysis can show patterns in the types of weaknesses being exploited in the organization and trends in its security posture, or help identify the root causes of security problems across the enterprise. These trends could show improvements or highlight repeating problem areas, for example

- increases or decreases in the number of vulnerabilities and incidents reported
- changes in the types of vulnerabilities and incidents being reported
- recurring vulnerabilities and incidents
- changes in the scope of an incident's impact
- targeted areas of the organization versus the entire organization

Results of trend analysis may be presented as reports to constituents or used to determine focused assistance. Information from trend analysis, if approved, can be released publicly or shared with other security groups.

Team Guidance

Team members should ensure that the trend analysis conducted also uses the results from other proactive analyses such as risk analysis, vulnerability scanning (VS), and system and network monitoring activities.

References

Regulatory References: None

[indirect]

FISMA Sec 3544 *Federal agency responsibilities* (b)(3) [OLRC 2003]

> "(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] to provide information security for the information and information systems that support the operations and assets of the agency […] that includes—
> (3) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate"

Guidance References: None

Organization Response

Examples of Evidence Sought			
❑ Copies of trend analysis reports ❑ Documentation of actions that were taken based on trend reports ❑ Tools or mechanisms used to correlate data ❑ Observations of correlation and trending activities ❑ Documentation of procedures describing how trending is done or which data streams are used ❑ Outputs from monitoring and other data collection and analysis tools			
Scoring Criteria	Yes	No	Evidence
Required			
3.3.2.01 Prerequisite: Data from events and incidents are available to support trend analysis.	❒	❒	
3.3.2.02 Control: Criteria exist for what should be captured, correlated, and synthesized in the trend analysis.	❒	❒	
3.3.2.03 Control: Personnel are appropriately trained on the relevant process, technology, and methodologies.	❒	❒	
3.3.2.04 Activity: Trend analysis is performed, including the results from other proactive risk analysis, vulnerability scanning, and network and system monitoring activities, if available.	❒	❒	
3.3.2.05 Activity: The analyses look for a variety of trends, such as • Changes in malicious activity • Types of weaknesses being exploited • Patterns in root causes • Changes in number of reported vulnerabilities and incidents • Recurring vulnerabilities and incidents • Targeted areas of the organization	❒	❒	
3.3.2.06 Activity: Trend analysis results are provided to designated individuals.	❒	❒	
3.3.2.07 Activity: Results of trend analysis are used to identify needed improvements to the security posture of organizational systems.	❒	❒	

Recommended Best Practices			
3.3.2.08 Activity: Automated trend analysis tools are used.	❒	❒	
Institutional and Quality Improvement			
3.3.2.09 Control: Documented procedures exist that detail how to perform trend analysis, disseminate information, and archive actions taken.	❒	❒	
3.3.2.10 Control: Personnel are aware of, knowledgeable of, and consistently perform the procedures for this activity.	❒	❒	
3.3.2.11 Quality: A process and criteria exist to evaluate how well this activity is performed and the quality of its artifacts.	❒	❒	
3.3.2.12 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒
Not Applicable		❒	**Not Observed**	❒

Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement
• Ensure that tested, automated tools are set up to support the collection of data for trend analysis in a consistent fashion.

- Provide training to incident management personnel on the best methods for performing trend analysis.

3.3 THREAT AND SITUATIONAL AWARENESS

3.3.3 Network and system configurations or rule sets are reviewed and updated in response to changes in the threat environment, and constituents are notified of the updates.

Priority I

Clarification

Failure to adjust network and system defenses to changes in threat environments could leave critical systems and data open to unauthorized access and exploitation. This capability focuses on whether the organization can quickly update and change network and system defense configurations and rule sets in a timely, structured manner to react to changes in the threat environment. It also ensures that incident management personnel receive threat information and changes in the threat environment and pass them to constituents and other stakeholders following agreed-upon standards or processes.

If incident management personnel do not perform this function, they should have an established interface with the authorized part of the organization that does. Such an interface enables them to easily pass on recommendations for preventing and responding to threats. Incident management personnel should also develop relationships and communication channels with other information sources that can provide indications of threat-change levels.

Team Guidance

It is possible for this capability to be handled by another part of the organization. In that case, this capability should be assessed and applied to that group and its activities.

References

Regulatory References: None

Guidance References:

[indirect]

NIST SP 800-41 Rev 1 *Guidelines on Firewalls and Firewall Policy* [Scarfone 2009]

> "This document seeks to assist organizations in understanding the capabilities of firewall technologies and firewall policies. It provides practical guidance on developing firewall policies and selecting, configuring, testing, deploying, and managing firewalls."

NIST SP 800-137 *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* [Dempsey 2010]

> "The purpose of this guideline is to assist organizations in the development of an ISCM strategy and the implementation of an ISCM program that provides awareness of threats and vulnerabilities, visibility into organizational assets, and the effectiveness of deployed security controls. The ISCM strategy and program support ongoing assurance that planned and implemented security controls are aligned with organizational risk tolerance, as well as the ability to provide the information needed to respond to risk in a timely manner."

Organization Response

Examples of Evidence Sought
❑ Documentation on when and why the latest rule sets were updated ❑ A change log for configuration updates ❑ Copies of change and impact notifications ❑ Up-to-date POC lists for constituents and stakeholders that receive notification of rule set changes ❑ Demonstrations or observations of vulnerability and threat monitoring mechanisms or methodologies ❑ Demonstrations or observations of information dissemination and communications mechanisms ❑ Demonstrations or observations of configuration and patch management systems, tools, or methodologies

Scoring Criteria	Yes	No	Evidence
Required			
3.3.3.01 Control: Documented guidance or requirements exist that define the types of changes in threat environments that require updates to configurations and rule sets.	❒	❒	
3.3.3.02 Control: Documented guidance or requirements exist that defines the process for gathering configuration/rule set update information and determining which actions to take.	❒	❒	
3.3.3.03 Control: Personnel are appropriately trained on the procedures, process, and supporting technologies (such as firewall rule sets, IDS, and router configurations) used to update network and system configurations and rule sets.	❒	❒	
3.3.3.04 Activity: Changes in the threat environment (e.g., threat and vulnerability reports and alerts) are monitored.	❒	❒	
3.3.3.05 Activity: Personnel analyze changes in the threat environment, determine recommended modifications to rule sets and configurations, and notify the appropriate group for implementation.	❒	❒	
3.3.3.06 Activity: The approved changes are implemented to IDS, router, firewall, and other appropriate network and system defense rules and configurations.	❒	❒	

3.3.3.07 Activity: Constituents are notified of approved modifications.	❒	❒	
Recommended Best Practices			
None	❒	❒	
Institutional and Quality Improvement			
3.3.3.08 Control: Documented procedures exist that define • what types of changes in threat environments require changes to configurations and rule sets, and the process for gathering that information and determining which actions to take • how to update router and firewall configurations (ACLs, logging, etc.) and IDS signatures • how to notify the organization of changes in the threat environment	❒	❒	
3.3.3.09 Control: A process and criteria exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	
3.3.3.10 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**		❒
Not Applicable		❒	**Not Observed**		❒
Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes
Suggestions for Improvement
None

3.3 THREAT AND SITUATIONAL AWARENESS

3.3.4 Penetration testing is conducted on organizational networks and systems.

Priority I

Clarification

This capability determines whether the organization conducts (or hires an independent third party to conduct) penetration testing on the constituent's networks and systems. Penetration testing (aka "pen testing") is defined in NIST SP 800-53 Rev 4 Appendix B as "A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system." Penetration testing may include laboratory based tests, red team exercises, or other forms of testing. Penetration testing typically is more invasive than the mere identification of vulnerabilities as performed in vulnerability assessments or vulnerability scanning (see capability 2.5.2). Penetration testing may use actual intruder exploits (although perhaps in a safer mode or with a less harmful payload, to minimize any disruptions or negative impacts) to defeat the security on the targeted networks or systems. Penetration testing of the network perimeter will make the organization aware of weaknesses that can be similarly identified or exploited by external actors. Penetration testing tools should be kept up to date with the latest known vulnerabilities, techniques, and exploits.

This activity can be performed by a CSIRT, by another part of the organization's incident management function, or by other divisions or branches within the constituency. It can also be done by external, third parties.

If penetration testing is performed by other divisions or branches in the constituency or by an external third party, incident management personnel might only perform tasks that involve providing to those other groups any information on implementing penetration testing methodologies and tools. Best practices recommend that the output of any penetration testing done by other divisions, branches, or external parties should be fed back to the CSIRT or incident management personnel.

If penetration testing is performed by the CSIRT or incident management personnel, processes and forms should be in place so that constituents can request penetration tests on a periodic or regular basis. The agreement between the CSIRT and the constituents should also outline what the results report contains.

If constituents perform the penetration testing activities themselves instead of incident management personnel, then they should discuss and agree to a best practice of sharing specific information with the incident management function. This information can be used by incident management personnel for analysis, correlation, and trending.

See NIST SP 800-53 Rev 4, Appendix F, control CA-2 (2) supplemental guidance (referenced below) for further information on a standard method for penetration testing.

Team Guidance

If constituents or external parties perform this function instead of incident management personnel, the assessment team should ensure that information is sent back to the incident management function and the personnel in the function are aware of the type and frequency of penetration testing being done.

Protect capability 2.5.2 is similar to this capability but is limited to vulnerability assessments and scanning. This capability on penetration testing goes beyond the mere identification and remediation of vulnerabilities; however it may include or build on vulnerability scanning as a preliminary activity. Per NIST 800-53, physical security controls should also be included in penetration testing.

It is possible that this capability might be marked N/A or not included in the assessment through scoping if no part of it is done by the incident management function.

References

Regulatory References: None

[indirect]

FISMA Sec 3544 *Federal agency responsibilities* (b)(5) [OLRC 2003]

> "(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] to provide information security for the information and information systems that support the operations and assets of the agency […] that includes— […]
>
> (5) periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually, of which such testing—
>
> (A) shall include testing of management, operational, and technical controls of every information system identified in the inventory required under section 3505(c); and
>
> (B) may include testing relied on in an evaluation under section 3545"

Guidance References:

NIST SP 800-53 Rev. 4 *Security and Privacy Controls for Federal Information Systems and Organizations* [NIST 2013]

> "Appendix F
>
> CA-2 Security Assessments
>
> Supplemental Guidance: […] Organizations can use other types of assessment activities such as vulnerability scanning and system monitoring to maintain the security posture of information systems during the entire life cycle. […]
>
> PE-3 Physical Access Control
>
> PE-3 (6) Physical Access Control | Facility Penetration Testing
>
> The organization employs a penetration testing process that includes [Assignment: organization-defined frequency], unannounced attempts to bypass or circumvent security controls associated with physical access points to the facility."

A Step-By-Step Approach on How to Set Up A CSIRT [ENISA, 2006]

> "A.2 CSIRT Services
>
> Penetration testing
>
> Testing the security of a site by purposefully attacking its systems and networks Obtaining upper management approval is required before conducting such audits or assessments. Some of these approaches may be prohibited by organizational policy. Providing this service can include developing a common set of practices against which the tests or assessments are conducted, along with developing a required skill set or certification requirements for staff

that perform the testing, assessments, audits, or reviews. This service could also be outsourced to a third part contractor or managed security service provider with the appropriate expertise in conducting audits and assessments."

Agency Response

Examples of Evidence Sought

- ❑ Authorization to perform penetration testing
- ❑ Examples of constituent request forms or written requests for assistance
- ❑ Copies of penetration testing results and analysis
- ❑ Demonstration or observation of penetration testing tools and methodologies

Scoring Criteria	Yes	No	Evidence
Required			
3.3.4.01 Control: Permission from management (or other authorization) exists to conduct penetration testing on the constituent networks and systems.	❒	❒	
3.3.4.02 Control: Documented policies exist requiring periodic (at organization-defined frequency) penetration testing of constituent networks and systems.	❒	❒	
3.3.4.03 Control: There is a defined process for penetration testing.	❒	❒	
3.3.4.04 Control: Personnel are appropriately trained on the processes, methods, and supporting technologies used to conduct penetration testing.	❒	❒	
3.3.4.05 Activity: Penetration testing assessments are conducted on constituent networks and systems.	❒	❒	
3.3.4.06 Activity: Penetration testing tools and methods are regularly updated to address new vulnerabilities and threats.	❒	❒	
3.3.4.07 Activity: Penetration testing tools and methods are tested and evaluated prior to their use on constituent networks and systems.	❒	❒	
3.3.4.08 Activity: Penetration testing results are analyzed, recorded, and tracked.	❒	❒	

3.3.4.09 Activity: Constituents are alerted to security deficiencies found in their networks or systems.	❒	❒	
3.3.4.10 Activity: Analysis includes a determination of what information about the systems and networks is discoverable by adversaries.	❒	❒	
Recommended Best Practices			
3.3.4.11 Control: Written authorization from management exists to conduct penetration testing on the constituent networks and systems	❒	❒	
3.3.4.12 Control: Existing documentation describes the penetration testing tools and methods, and their potential impact on constituent networks and systems.	❒	❒	
3.3.4.13 Control: If penetration testing is performed by constituents, the results are forwarded to incident management personnel for further analysis or trending.	❒	❒	
3.3.4.14 Control: If penetration testing is performed by incident management personnel, a method for constituents to request this service is documented and followed.	❒	❒	
3.3.4.15 Activity: Results of this activity are archived in a secure and protected manner.	❒	❒	
3.3.4.16 Activity: Lessons learned from penetration testing are incorporated into future penetration testing processes and training.	❒	❒	
Institutional and Quality Improvement			
3.3.4.17 Control: Documented procedures exist that describe the process and method used to obtain permission for penetration testing on organizational systems.	❒	❒	
3.3.4.18 Control: Documented procedures exist that define the process and method used to perform penetration testing.	❒	❒	
3.3.4.19 Control: Documented procedures exist that define the process and method used to analyze results gathered from penetration testing.	❒	❒	
3.3.4.20 Quality: Personnel are aware of, knowledgeable of, and consistently follow or use the procedures, processes, methodologies, and technologies for performing this task.	❒	❒	

3.3.4.21 Quality: A process and criteria exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	
3.3.4.22 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒
Not Applicable		❒	**Not Observed**	❒

Evidence Collected

Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement

None

RESPOND: SECTION 4 OF INCIDENT MANAGEMENT CAPABILITIES

In Respond, information that was received by incident management personnel concerning potential incidents, vulnerabilities, or other computer security events is acted on. These actions include those that may be performed by technical staff, management, or other entities within an organization. For example, technical actions can include

- analyzing the event or incident information, data, and supplemental material such as log files, malicious code, or other artifacts
- researching corresponding mitigation strategies and recovery options
- developing advisories, alerts, and other publications that provide guidance and advice for resolving or mitigating the event or incident
- containing any ongoing malicious activity by making technical changes to the infrastructure, such as disconnecting affected systems from the network, changing security configurations, or filtering ports, services, IP addresses, or packet content via firewalls, mail servers, routers, or other devices
- eradicating or cleaning up any malicious exploits, processes, or files
- repairing or recovering affected systems
- providing assistance to constituents regarding response actions

Depending on the scope of the event or incident being handled, actions in Respond may be performed by a variety of people. For example, a CSIRT may perform initial incident analysis activities and provide guidance on responding to the incident but not be involved in performing containment, eradication, or recovery actions within the infrastructure. IT staff members or local system administrators may make those changes. Because all actions are in response to ongoing incident activity, they are considered part of the incident management function.

From a different perspective, management response focuses on activities that require some type of supervisory or management intervention, notification, interaction, escalation, or approval as part of any response that is undertaken. Such management involvement may include actions taken by executive management or functional business managers such as HR, legal counsel, public relations, financial accounting, audits and compliance, and other internal organizational entities. Management response can also involve ensuring that various parts of the organization work together to handle events and incidents, and resolving any problems that occur between different parts of the organization.

Coordination must occur across all areas of Respond to be efficient and effective. All those involved in the response must communicate the steps that are being taken and any relevant information that needs to be disseminated. A response, such as a technical response, may require others to be involved. This type of cooperation and coordination should occur through established channels of communication that should be outlined in the policies, procedures, and plans associated with Respond. Actions are coordinated to ensure that efforts are not duplicated and all tasks are completed within agreed upon timeframes.

The Respond category includes the following subcategories and capabilities:

4.1. Incident Reporting—Incident management personnel and constituency understand the requirements for reporting and notification; information is appropriately managed, accessed, stored, archived, or destroyed.

4.1.1. Events and incidents are reported from the constituency.

4.1.2. Incidents are reported to appropriate management in accordance with organizational guidelines.

4.1.3. Incidents are reported to and coordinated with the appropriate external organizations or groups in accordance with organizational guidelines.

4.1.4. Incident management is supported for restricted information, networks, and systems.

4.2. Analysis—This analysis is conducted to determine the scope and impact of reported events and incidents, and to determine the appropriate response strategies or workarounds to provide resolution or mitigation.

4.2.1. Incident management personnel conduct triage of events and incidents.

4.2.2. Incident analysis is performed on declared incidents.

4.2.3. Incident correlation is performed to identify similar activity.

4.2.4. Impact of an incident is determined.

4.2.5. Incident root cause analysis is conducted.

4.2.6. Fusion analysis is performed to identify concerted attacks and shared vulnerabilities.

4.2.7. Retrospective analysis is conducted.

4.2.8. Media analysis is performed on constituent networks and systems.

4.2.9. Artifact or malware analysis is conducted.

4.3. Incident Response—A 24/7 response capability exists, and effective response processes are implemented, including involvement of appropriate individuals from technical, management, legal, and other areas of the organization as required. Information is tracked and recorded, guidance is provided to organizational business units on how to report, and incident management personnel build trusted relationships with internal organization experts and other external experts to facilitate response activities.

4.3.1. General incident response guidance and procedures are distributed to constituents.

4.3.2. Incidents are resolved.

4.3.3. Incident management personnel coordinate incident response across stakeholders.

4.3.4. Incident management personnel create alerts and warnings, and distribute them as needed.

4.3.5. Incident management personnel verify that a response is implemented, as appropriate, and that the incident is closed, in accordance with organizational guidance.

4.3.6. Postmortem reviews of significant incidents are conducted, and lessons learned are identified and acted upon, as appropriate.

4.1 INCIDENT REPORTING

4.1.1 Events and incidents are reported from the constituency. **Priority I**

Clarification

This capability focuses on the events and incidents being reported from the constituents. For this activity to occur efficiently, defined, easy-to-use mechanisms for reporting events and incidents should exist. These mechanisms need to be advertised along with instructions for their use. Such mechanisms facilitate the transfer of appropriate and useful information. Incident reporting guidelines indicate what needs to be reported, to whom, when, why, and how. These guidelines should also be readily available.

Team Guidance

The team should look for evidence that incidents are being reported, either directly to the incident management function or indirectly through other groups such as the IT helpdesk or a business unit. The team should determine that incident management personnel are familiar with reporting requirements, understand the types of activity to be reported (e.g., categories, reporting criteria, priorities, thresholds/triggers), and follow the guidance on reporting. By inference, the team should determine that the constituency has access to the reporting requirements, guidelines, and mechanisms by reviewing actual event or incident reports from inside the organization and evaluating adherence to those requirements and guidelines. The team should also look for evidence that the information reported is done according to the level of security required and is properly stored and handled.

References

Regulatory References:

FISMA Sec 3544 *Federal agency responsibilities* (b)(7) [OLRC 2003]

> "(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] that includes— […]
> (7) procedures for detecting, reporting, and responding to security incidents […]"

Guidance References:

NIST SP 800-61 Rev 2 *Computer Security Incident Handling Guide* [Cichonski 2012]

> "Sec 2.3.1 Policy Elements
>
> […] requirements for reporting certain kinds of incidents
>
> Sec 2.6 Recommendations
>
> Create an incident response policy. The incident response policy is the foundation of the incident response program. It defines which events are considered incidents, establishes the organizational structure for incident response, defines roles and responsibilities, and lists the requirements for reporting incidents, among other items.
>
> Sec 3.5 Incident Handling Checklist
>
> Table 3-5. Generic Incident Handling Checklist

Action 3

Report the incident to the appropriate internal personnel and external organizations.

Sec 3.6 Recommendations

Include provisions regarding incident reporting in the organization's incident response policy. Organizations should specify which incidents must be reported, when they must be reported, and to whom. The parties most commonly notified are the CIO, head of information security, local information security officer, other incident response teams within the organization, and system owners."

Expectations for Computer Security Incident Response [NWG 1998]

"3.5.1.2 Incident Coordination

Incident Coordination normally includes:

d) Information categorization

e) Categorization of the incident related information (log files, contact information, etc.) with respect to the information disclosure policy.

- Coordination Notification of other involved parties on a need-to-know basis, as per the information disclosure policy."

Organization Response

Examples of Evidence Sought

- ❑ Copies of reports received from individuals or constituents within the organization
- ❑ Forms/mechanisms used to report organizational events/incidents, with instructions and examples (e.g., email, web forms/instructions)
- ❑ Documented and up-to-date organizational POC lists with appropriate contact information and alternates
- ❑ Observation of events or incidents being reported to the incident management function from within the organization

Scoring Criteria	Yes	No	Evidence
Required			
4.1.1.01 Control: A policy or guidance exists that defines what types of events/incidents should be reported.	❒	❒	
4.1.1.02 Control: Guidance is provided to constituents on how events and incidents should be reported.	❒	❒	
4.1.1.03 Activity: Incident management personnel receive event and incident reports from constituents.	❒	❒	
4.1.1.04 Activity: Event/incident reports are reviewed, and a decision is made about how to respond.	❒	❒	

Recommended Best Practices			
4.1.1.05 Control: Defined reporting agreements (e.g., MOUs, SLAs, policies, guidance, general knowledge) between constituents and the IM function specify any data or information that must be excluded, sanitized, abstracted, or access-limited.	❒	❒	
4.1.1.06 Activity: Regular review of reporting guidelines with the organization is performed, and guidelines are updated as needed.	❒	❒	
Institutional and Quality Improvement			
4.1.1.07 Control: Documented procedures exist for the constituents' reporting of events and incidents (including criteria for what events/incidents to report, how to report, required content for the report, and required timeframes).	❒	❒	
4.1.1.08 Quality: Personnel are aware of, knowledgeable of, and consistently follow the procedures for this activity.	❒	❒	
4.1.1.09 Quality: A process and criteria exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	
4.1.1.10 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒
Not Applicable		❒	**Not Observed**	❒

Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement
• Provide feedback regarding incident and vulnerability trends seen in the organization based on reports and on proactive network monitoring to show the benefit of reporting accurate and timely information. • Be selective about the information required for constituent reporting. If too much information is required from constituents in the organization, they may be discouraged from reporting. If too little information is required, incident management personnel will waste time contacting organizations to get additional data.

4.1 INCIDENT REPORTING

4.1.2 Incidents are reported to appropriate management in accordance with organizational guidelines.

Priority I

Clarification

This capability ensures that incident management personnel follow organizational guidelines in reporting incidents and events within the organization. The objective is to be able to demonstrate that appropriate notification is made to organizational management using a repeatable, consistent, and reliable process that is well-documented, up-to-date, and understood by members of the team.

Note that another capability (4.3.4, under Incident Response) addresses the providing of alerts and warnings to the general organization, as needed. Several of the indicators in this capability are similar to or may overlap with those in capability 4.3.4, however this capability focuses specifically on reporting incidents and events to appropriate management groups within the organization.

Team Guidance

The team should look for evidence that IM personnel are following organizational management's requirements for guidance on reporting. Rather than reporting directly to management, the team may report to a designated POC (e.g., ISO, CIO, chief information security officer [CISO]). Reporting could also be made to the management of the affected system owners, business units, and management of other groups when appropriate (e.g., HR, Public Affairs, or Legal department).

References

Regulatory References: None

Guidance References:

NIST SP 800-61 Rev 2 *Computer Security Incident Handling Guide* [Cichonski 2012]

> "Sec 3.2.7 Incident Notification
> When an incident is analyzed and prioritized, the incident response team needs to notify the appropriate individuals so that all who need to be involved will play their roles. Incident response policies should include provisions concerning incident reporting—at a minimum, what must be reported to whom and at what times (e.g., initial notification, regular status updates).
>
> Sec 3.5 Incident Handling Checklist
>
> Table 3-5. Incident Handling Checklist
>
> Action 3.
>
> Report the incident to the appropriate internal personnel and external organizations.
>
> Sec 3.6 Recommendations
>
> Include provisions regarding incident reporting in the organization's incident response policy. Organizations should specify which incidents must be reported, when they must be reported, and to whom. The parties most commonly notified are the CIO, head of information security,

local information security officer, other incident response teams within the organization, and system owners."

Organization Response

Examples of Evidence Sought

- ❑ Copies of reports to management or designated reporting POCs
- ❑ Records of how long it took to report incidents to management
- ❑ Documented and up-to-date executive and business management POC lists with appropriate contact information and alternates
- ❑ Defined mechanisms (e.g., forms, email, telephone) used for incident reporting and notification, with instructions and examples
- ❑ Secure communications mechanisms, which are used to quickly disseminate incident and vulnerability information to organizational stakeholders and business units, commensurate with the sensitivity of the information (e.g., PGP, GnuPG, Secure/Multipurpose Internet Mail Extensions [S/MIME], public key infrastructure [PKI], secure terminal equipment [STE], secure FAX, secure portal)

Scoring Criteria	Yes	No	Evidence
Required			
4.1.2.01 Control: Organizational guidance (including criteria for what incidents to report, how to report, required content for reporting, and required timeframes) exists for internal reporting of incidents to organizational management.	❒	❒	
4.1.2.02 Control: A policy or guidance exists that defines what types of incidents should be reported and to whom.	❒	❒	
4.1.2.03 Control: Personnel are appropriately trained in the processes and relevant mechanisms for reporting to or notifying management.	❒	❒	
4.1.2.04 Activity: Management is notified about incidents according to policy and guidance.	❒	❒	
4.1.2.05 Activity: Sensitive and classified information is handled and stored according to Federal and organizational requirements.	❒	❒	
Recommended Best Practices			
4.1.2.06 Control: Documented requirements exist for levels of communications security.	❒	❒	

4.1.2.07 Activity: The reporting guidelines are reviewed at least annually with organizational management and updated as needed.	❒	❒	
Institutional and Quality Improvement			
4.1.2.08 Control: Documented procedures exist for reporting incidents internally to organizational management.	❒	❒	
4.1.2.09 Quality: Personnel are aware of, knowledgeable of, and consistently follow the procedures for this activity.	❒	❒	
4.1.2.10 Quality: A process and criteria exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	
4.1.2.11 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒
Not Applicable		❒	**Not Observed**	❒

Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement
None

4.1 INCIDENT REPORTING

4.1.3 Incidents are reported to and coordinated with the appropriate external organizations or groups in accordance with organizational guidelines.

Priority I

Clarification

This capability is concerned with external incident reporting and coordination. The primary focus is the timely reporting of incidents to appropriate contacts in other organizations or groups. The incident management function may report externally for a variety of reasons, including mandated reporting of specific types of information, information sharing, or broader situational awareness. For example, FISMA requires Federal government agencies to report security incidents to US-CERT [OLRC 2003]. The external groups also include LE and the intelligence community (IC) as appropriate. In addition, coordination with these groups or other CSIRTs to exchange and compare information is addressed here, although it is not a required activity. Some organizations in specific domains may have requirements for reporting incidents to a central reporting organization or may be part of a voluntary group of organizations pooling their incident information for greater effect. Some organizations may be required through Federal, state, or local compliance regulations or laws to report certain types of incidents such as unauthorized released of personally identifiable information (PII) to other organizations and to data owners.

Information reported should include the timeframes, details, and any other relevant information. For example, coordinating centers provide incident reporting guidelines on their websites. Note that LE may have different reporting requirements than the IC so it's important for an organization to determine when it should report to either area and be aware of the exact reporting process and POCs. It's also important for the organization to have clear guidance on how this reporting is to be performed so the right information gets to the right people at the right time.

Note that this capability is related to other response capabilities for reporting incidents to management (see capability 4.1.2) and providing alerts and warnings (see capability 4.3.4).

Team Guidance

The team should look for evidence that the IM function not only understands the requirements for reporting and coordination, but also submits requisite reports and shares information in a consistent, accurate, timely, and complete manner.

The team should be familiar with current incident reporting requirements and guidelines, as provided by CERT/CC, and any other applicable external organizations. For example, CERT/CC incident reporting guidelines, including definitions and reporting timeframes, are posted at *http://www.us-cert.gov/government-users/reporting-requirements.*

Reporting to the IC may not always be a requirement for some organizations. Indirect reporting and communication may occur through an intermediate legal representative or senior management. In those cases, this capability only applies to the incident management personnel for reporting to the intermediate group/person.

References

Regulatory References:

FISMA Sec 3544 *Federal agency responsibilities* (b)(7)(B) [OLRC 2003]

"(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] to provide information security for the information and information systems that support the operations and assets of the agency […] that includes— […]

(7) procedures for detecting, reporting, and responding to security incidents […] including— […]

(B) notifying and consulting with the Federal information security incident center referred to in section 3546 [US-CERT]

(C) notifying and consulting with, as appropriate—

(i) law enforcement agencies and relevant Offices of Inspector General"

Memorandum M-07-16 *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* [OMB 2007]

[p 10]

"Agencies must report all incidents involving personally identifiable information to US-CERT. This reporting requirement does not distinguish between potential and confirmed breaches.

For incidents involving personally identifiable information, agencies must: […]

Notify the issuing bank if the breach involves government-authorized credit cards; and

Notify US-CERT within one hour."

Guidance References:

NIST SP 800-61 Rev 2 *Computer Security Incident Handling Guide* [Cichonski 2012]

"Sec 2.3.4 Sharing Information With Outside Parties
Organizations often need to communicate with outside parties regarding an incident, and they should do so whenever appropriate, such as contacting law enforcement, fielding media inquiries, and seeking external expertise. Another example is discussing incidents with other involved parties, such as Internet service providers (ISPs), the vendor of vulnerable software, or other incident response teams. […]

Sec 2.3.4.2 Law Enforcement
The incident response team should become acquainted with its various law enforcement representatives before an incident occurs to discuss conditions under which incidents should be reported to them, how the reporting should be performed, what evidence should be collected, and how it should be collected.
Law enforcement should be contacted through designated individuals in a manner consistent with the requirements of the law and the organization's procedures.

Sec. 2,3,4,3

FISMA requires Federal agencies to report incidents to United States Computer Emergency Readiness Team (US-CERT) […]
Sec 2.3.4.4 Other Outside Parties
An organization may want to discuss incidents with other groups, including those listed below.

- Organization's ISP. […]
- Owners of Attacking Addresses. […]
- Software Vendors. […]

- Other Incident Response Teams. […]
- Affected External Parties. […]

OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, requires Federal agencies to develop and implement a breach notification policy for personally identifiable information (PII)."

NIST SP 800-53 Rev. 4 Security and Privacy Controls for Federal Information Systems and Organizations [NIST 2013]

"IR-6 INCIDENT REPORTING

Control: The organization:

(b.) Reports security incident information to [*Assignment: organization-defined authorities*]."

Organization Response

Examples of Evidence Sought

- ❑ Copies of reports sent to other external organizations or CSIRTs
- ❑ Copies of reports to LE, the IC, or an intermediate group
- ❑ Confirmation receipts from other external organizations when applicable
- ❑ Forms (e.g., paper, email, web), templates, or tools, including instructions or examples, for reporting incidents to external organizations
- ❑ Observations or demonstrations of communication channels or mechanisms for reporting
- ❑ Documented, accurate POC lists for other CSIRTS or internal incident management personnel or groups
- ❑ Secure communications mechanisms to report incident or vulnerability information to the appropriate external organizations in a manner that is commensurate with the sensitivity of the information (e.g., encrypted email, PGP/GnuPG, S/MIME, PKI, STE, secure FAX, secure portal, Joint Worldwide Intelligence Communications System [JWICS], Secret Internet Protocol Router Network [SIPRNET])

Scoring Criteria	Yes	No	Evidence
Required			
4.1.3.01 Control: A documented policy or guidance exists that includes the categories of incidents to report, the required information, timeframes, and contact mechanisms.	❒	❒	
4.1.3.02 Control: A department, group, or manager in the organization is designated as having responsibility for reporting incidents to LE, IC[21], and any designated coordinating CSIRTs, if appropriate.	❒	❒	

[21] There may be only one designee, or each entity may have its own designee.

4.1.3.03 Control: Criteria and guidance exist for reporting incidents and coordinating/exchanging information with other CSIRTS or other security organizations.	❒	❒	
4.1.3.04 Control: A documented policy or guidance exists for reporting incidents and coordinating/exchanging information with LE and IC.	❒	❒	
4.1.3.05 Control: Personnel are appropriately trained on how to notify other organizations, other CSIRTs, LE, IC, security organizations, and any designated coordinating CSIRTs.	❒	❒	
4.1.3.06 Activity: The organization reports the appropriate types of incidents to other external organizations, such as LE, IC, or any designated coordinating CSIRTs, in accordance with organizational guidelines.	❒	❒	
4.1.3.07 Activity: The organization reports incidents involving PII breaches to the appropriate entities in accordance with any relevant security breach notification laws and organizational guidelines.	❒	❒	
Recommended Best Practices			
4.1.3.08 Activity: Confirmation of reported incidents is received from external organizations when applicable.	❒	❒	
4.1.3.09 Activity: Coordination with other CSIRTS and security organizations occurs to compare and exchange notes, analysis reports, and other information on intrusions, attacks, and suspicious activities within organizational guidelines.	❒	❒	
4.1.3.10 Activity: Personnel participate in workshops, conferences, working groups, technical exchanges, and so forth to improve communication channels with external organizations (other organizations, other CSIRTs, LE, etc.).	❒	❒	
Institutional and Quality Improvement			
4.1.3.11 Control: Documented procedures exist for reporting incidents to other relevant organizations, including assigned roles, responsibilities, updated POCs, information-sharing channels, requirements for evidence handling, incident categories, and associated reporting requirements.	❒	❒	
4.1.3.12 Quality: Personnel are aware of, knowledgeable of, and consistently follow the procedures for this activity.	❒	❒	

4.1.3.13 Quality: A process and criteria exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	
4.1.3.14 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒
Not Applicable		❒	**Not Observed**	❒

Evidence Collected

Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement

- Have a cost-effective means of meeting reporting requirements (e.g., automated tools, templates). Implementing a centralized incident database that can automatically produce the required reports is an example of such an improvement. Provide templates or forms to ensure consistent reporting if templates are not provided by the external organization.
- Meet with LE personnel in advance of any need to report events or incidents so you understand their requirements for reporting.

4.1 INCIDENT REPORTING

4.1.4 Incident management is supported for restricted information, networks, and systems.

Priority I

Clarification

In the course of incident response activities, incident management personnel may need to handle restricted or other sensitive data (confidential, proprietary, or other restricted information). They must be ready to receive, transmit, and store such information according to constituent organizational classification schemes commensurate with the data's sensitivity. This requirement means that

- designated personnel have the appropriate clearances to receive such information
- approved secure communications mechanisms exist, and email encryption tools, and are available to incident management and constituent staff
- personnel are trained in the handling of sensitive information and the tools to use
- appropriate secure facilities, such as sensitive compartment information facilities (SCIFs) or secure rooms, can be accessed within designated time constraints by personnel designated to handled such data

The constituents and stakeholders also need to know how to properly report events and incidents that involve sensitive or restricted information, systems, or networks; and how to receive sensitive information from incident management or CSIRT personnel. Therefore, guidance and instructions should be available to them.

Team Guidance

The assessment team will likely need appropriate clearances to be able to view, confirm, and validate that the capability has been satisfied. Policies for incidents involving classified or sensitive information or networks should include who is to be notified, who can deal with the incident, the type of information to be collected, and other constraints.

The team should verify the incident management personnel who handle such data have the appropriate clearances, training, facilities, and equipment.

References

Regulatory References:

FISMA Sec 3544 *Federal agency responsibilities* (b)(7) [OLRC 2003]

> "(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] to provide information security for the information and information systems that support the operations and assets of the agency […] that includes— […]
>
> (7) procedures for detecting, reporting, and responding to security incidents, consistent with standards and guidelines issued pursuant to section 3546(b) [National Security Systems] […]"

Guidance References: None

[indirect]

NIST SP 800-59 *Guideline for Identifying an Information System as a National Security System* [Barker 2003]

> "This document provides guidelines developed in conjunction with the Department of Defense, including the National Security Agency, for identifying an information system as a national security system. The basis for these guidelines is the Federal Information Security Management Act of 2002 (FISMA, Title III, Public Law 107-347, December 17, 2002), which provides government-wide requirements for information security, superseding the Government Information Security Reform Act and the Computer Security Act."

Organization Response

Examples of Evidence Sought

- ❑ Observations of restricted levels being clearly marked on reports
- ❑ Observations that restricted reports are stored at their level of sensitivity
- ❑ Observations or demonstrations of secure communication channels at the for incidents involving restricted or sensitive information
- ❑ Defined ACLs for associated levels of restriction or sensitivity (e.g., who has authorized access to what)
- ❑ Secure storage or a repository appropriate to the levels of sensitivity
- ❑ Encryption techniques that meet NIST or other national or international regulations
- ❑ A decision matrix or mechanism used for quickly assigning the proper restriction or disclosure guidance to event and incident data and reports
- ❑ Observations of one or more secure facilities used for secure communication and storage

Scoring Criteria	Yes	No	Evidence
Required			
4.1.4.01 Control: An inventory exists of restricted or sensitive networks and systems used by constituents.	❒	❒	
4.1.4.02 Control: Defined levels/schemes of sensitivity/restrictions for data and information exist as appropriate.	❒	❒	
4.1.4.03 Control: Documented requirements exist for levels of communication security.	❒	❒	
4.1.4.04 Control: A documented policy exists for managing incidents that involve networks or systems supporting sensitive or restricted information.	❒	❒	

4.1.4.05 Control: Personnel are cleared to handle the sensitivity levels of networks, systems, and information as appropriate for their jobs.	❒	❒	
4.1.4.06 Control: Personnel are trained appropriately in processes and relevant technology.	❒	❒	
4.1.4.07 Activity: Incidents involving sensitive or restricted information are handled according to organizational and constituent guidelines and policies.	❒	❒	
4.1.4.08 Activity: Data and information have been assigned and labeled according to the appropriate class or category of sensitivity.	❒	❒	
4.1.4.09 Activity: Incidents involving sensitive or restricted information are stored in approved facilities according to the appropriate organizational and constituent guidelines.	❒	❒	
Recommended Best Practices			
4.1.4.10 Control: Cleared personnel who can perform incident management actions for restricted or sensitive data, systems, or networks are available or on-call at all times and can access secure communications mechanisms within 30 minutes.	❒	❒	
4.1.4.11 Quality: Clearance records for personnel are on file.	❒	❒	
Institutional and Quality Improvement			
4.1.4.12 Control: Documented procedures exist that cover all aspects of managing incidents involving restricted or sensitive information, networks, or systems, including • the response • external and internal reporting • the required means of communicating • specified markings for levels of sensitivity • variations for different levels of sensitivity • the use of encryption • the use of secure communication channels	❒	❒	
4.1.4.14 Control: Personnel are aware of, knowledgeable of, and consistently perform the procedures for incidents involving sensitive or restricted information.	❒	❒	

4.1.4.15 Quality: A process and criteria exist for evaluating the quality of performance and artifacts associated with this activity.	❒	❒	
4.1.4.16 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒
Not Applicable		❒	**Not Observed**	❒

Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement
None

4.2 ANALYSIS

4.2.1 Incident management personnel conduct triage of events and incidents.

Priority I

Clarification

This capability focuses on whether the organization employs a deliberate triage process or as part of some other incident management process. The purpose of triage is to screen/sort, correlate, and categorize events and incidents in order to prioritize them for further response actions. This enables effective usage of incident management resources and a timely response to more critical events and incidents. Triage is particularly needed in order to identify those events and incidents where rapid response is essential.

Triage may also include the initial assignment of further response to a particular group or individual. Although later analysis may necessitate a change in an incident's categories or priority, triage concentrates on the initial categorization and prioritization for the incident to be assigned to the appropriate personnel and receive the most efficient response.

Incident categories and priorities should be predefined (refer to capability 1.2.6).

Note that a separate capability (4.2.3) focuses on cross-incident correlation, which can facilitate the triage process.

Team Guidance

The assessment team should determine that the IM function not only understands the requirements and methodologies for performing incident triage, but also performs triage in a consistent, accurate, and timely manner. Triage is a process that needs to be supported 24x7. The assessment team should also examine the process by which triage data is received and disseminated after analysis.

The triage process does not have to exist by itself with dedicated staff. Triage may be part of one of several processes in an organization, including help-desk activity or incident analysis.

A CSIRT may take the lead in performing incident triage, but other staff in the organization, (IT helpdesk, SOC, etc.) who have the required skills and expertise might do triage instead. In that case, this capability should also be applied to other groups that perform this function.

References

Regulatory References: None

Guidance References:

NIST SP 800-61 Rev 2 *Computer Security Incident Handling Guide* [Cichonski 2012]

> "Sec. 3.3.6 Incident Prioritization
>
> [p 32-33] "Prioritizing the handling of the incident is perhaps the most critical decision point in the incident handling process. Incidents should not be handled on a first-come, first-served basis as a result of resource limitations. Instead, handling should be prioritized based on the relevant factors, such as the following:
>
> Functional Impact of the Incident. […]

Information Impact of the Incident. […]

Recoverability from the Incident. […]

An organization can best quantify the effect of its own incidents because of its situational awareness."

NIST SP 800-53 Rev. 4 *Security and Privacy Controls for Federal Information Systems and Organizations* [NIST 2013]

"IR-4 INCIDENT HANDLING

Control: The organization:

(a.) Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery […]

Control Enhancements:

(1.) […]

(2.) […]

(3.) The organization identifies [Assignment: organization-defined classes of incidents] […] Enhancement Supplemental Guidance: Classes of incidents include, for example, malfunctions due to design/implementation errors and omissions, targeted malicious attacks, and untargeted malicious attacks. […]

(4.) The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response."

Organization Response

Examples of Evidence Sought

- ❑ Sample incident categories with definitions or descriptions
- ❑ Sample prioritization categories with definitions or descriptions
- ❑ Documented procedures or processes for performing triage
- ❑ Criteria for categorizing and prioritizing incidents
- ❑ Observation of personnel performing triage
- ❑ Observation or demonstration of tools supporting triage

Scoring Criteria	Yes	No	Evidence
Required			
4.2.1.01 Prerequisite: Incident information from other reports is available to and accessible by triage personnel who perform categorization and prioritization.	❒	❒	

4.2.1.02 Control: Guidance or processes exist for conducting triage on incidents.	❒	❒	
4.2.1.03 Control: Personnel are trained appropriately in the processes and relevant technology.	❒	❒	
4.2.1.04 Activity: Categorization and prioritization of events and incidents is determined during the triage process.	❒	❒	
4.2.1.05 Activity: Incidents are escalated according to defined guidance.	❒	❒	
4.2.1.06 Activity: The mechanism by which incidents are escalated from the triage process is documented and maintained.	❒	❒	
4.2.1.07 Activity: A responsible person with needed skills is assigned to handle an incident after triage is completed.	❒	❒	
Recommended Best Practices			
4.2.1.08 Control: Tools are installed to assist and ensure accuracy and consistency in the triage process.	❒	❒	
4.2.1.09 Activity: Intra-incident correlation is performed.	❒	❒	
4.2.1.10 Activity: Advanced tools are used for automated correlation.	❒	❒	
4.2.1.11 Activity: Triage is conducted on incident reports regardless of the time they are received.	❒	❒	
Institutional and Quality Improvement			
4.2.1.12 Control: Documented procedures exist that cover all aspects of the triage process, including • incident categories • incident priorities • correlation criteria • assignment of further analysis or response to specific groups or individuals	❒	❒	
4.2.1.13 Control: Personnel are aware of, knowledgeable of, and consistently perform the procedures.	❒	❒	

4.2.1.14 Quality: A process and criteria exist for evaluating the quality of performance and artifacts associated with this activity.	❒	❒	
4.2.1.15 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒
Not Applicable		❒	**Not Observed**	❒

Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement
None

4.2 ANALYSIS

4.2.2 Incident analysis is performed on declared incidents. **Priority I**

Clarification

There are many different types of analysis that can be done during the incident management lifecycle. Analysis ranges from various malware analysis methodologies, to media analysis as part of forensics work, to correlation and trending. Each of these is a distinct type of analysis. Not all of these forms of analysis are conducted for ever event or incident, only those where such methods are relevant.

However, there is a basic type of analysis, "incident analysis" that should be performed on events that meet the criteria or threshold to be declared incidents. This basic analysis focuses on collecting and reviewing information regarding the *who*, *what*, *where*, and *when* of an incident to determine the extent of the threat and resulting damage.

The purpose of the analysis is to identify the scope and nature of the incident, the involved parties, and the timeframe, the relationship of the incident to other activities, and available response strategies or workarounds. Incident analysis can also answer questions concerning whether the incident is ongoing or is over and whether it was successful or not.

Incident management personnel may use the results of vulnerability, media, and artifact analysis to supplement incident analysis and provide more complete and up-to-date insight into what happened on a specific system or network.

Team Guidance

The team should determine that the IM function not only understands the requirements and methodologies for performing incident analysis, but also performs the analysis in a consistent, accurate, timely, and complete manner. This function can be performed by various parts of an organization's incident management staff, including a CSIRT, SOC, crisis team, or any other group that has the required skills and expertise. The team should identify what part of the organization performs the incident analysis capability and address this set of indicators to them. It is possible that more than one group performs this function. If so, then this capability should be addressed to each involved group.

Remember that this capability addresses ONLY incident analysis and does not pertain to other types of analysis such as malware, media, or vulnerability analysis which are their own capabilities. It also does not pertain to correlation, trending, retrospective, historic, or fusion analysis, which are also their own capabilities. Finally it does not pertain to root cause analysis or impact analysis which are also their own capabilities.

References

Regulatory References: None

Guidance References:

NIST SP 800-61 Rev 2 *Computer Security Incident Handling Guide* [Cichonski 2012]

> "Sec 3.2.4 Incident Analysis
>
> […] each indicator ideally should be evaluated to determine if it is legitimate.

Incident handlers are responsible for analyzing ambiguous, contradictory, and incomplete symptoms to determine what has happened. […]"

[indirect]

"Sec 3.2.5 Incident Documentation
An incident response team that suspects that an incident has occurred should immediately start recording all facts regarding the incident."

NIST SP 800-53 Rev. 4 *Security and Privacy Controls for Federal Information Systems and Organizations* [NIST 2013]

"IR-4 INCIDENT HANDLING

Control: The organization:

(b.) Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;"

A Step-by-Step Approach on How to Set Up A CSIRT [ENISA, 2006]

"A.2 CSIRT Services

Incident analysis

There are many levels of incident analysis and many sub-services. Essentially, incident analysis is an examination of all available information and supporting evidence or artifacts related to an incident or event. The purpose of the analysis is to identify the scope of the incident, the extent of damage caused by the incident, the nature of the incident, and available response strategies or workarounds. The CSIRT may use the results of vulnerability and artifact analysis (described below) to understand and provide the most complete and up-to-date analysis of what has happened on a specific system. The CSIRT correlates activity across incidents to determine any interrelations, trends, patterns, or intruder signatures. Two sub-services that may be done as part of incident analysis, depending on the mission, goals, and processes of the CSIRT, are Forensic evidence collection…Tracking or tracing"

Good Practice Guide for Incident Management [ENISA, 2010]

"8.4.1 Data analysis
To start data analysis, first you have to notify the parties involved and collect data from them. First you inform those who may be the most affected. You may include in this notification some initial advice and information about further proceedings to resolve the incident. You should collect as much data as possible. There are several main sources of such data: […]"

Organization Response

Examples of Evidence Sought

- ❑ Documented procedures or process guidance for performing incident analysis.
- ❑ Sample incident analysis findings included within incident tracking system or as stand-alone reports
- ❑ Sample recommendations for remediation or countermeasures
- ❑ Observation or demonstration of incident management staff performing incident analysis
- ❑ Observation or demonstration of tools supporting incident analysis
- ❑ Observation or demonstration of incident tracking systems containing analysis results

Scoring Criteria	Yes	No	Evidence
Required			
4.2.2.01 Control: An incident analysis process exists.	❒	❒	
4.2.2.02 Control: Personnel are appropriately trained on the relevant process, technology, and methodologies.	❒	❒	
4.2.2.03 Activity: Incident analysis is performed on incidents that meet organizational thresholds or criteria.	❒	❒	
4.2.2.04 Activity: Analysis is conducted at the level and type of analysis appropriate to the incident's category and severity.	❒	❒	
4.2.2.05 Activity: Incident analysis results are used to help develop recommendations and countermeasures to address the incidents.	❒	❒	
4.2.2.06 Activity: The results of incident analysis are documented as part of the incident information in the organizational incident tracking system.	❒	❒	
Recommended Best Practices			
4.2.2.07 Activity: Incident analysis results are provided to the affected constituents according to organizational guidelines.	❒	❒	
4.2.2.08 Activity: Sanitized information is provided to other constituents or external contacts as appropriate.	❒	❒	
Institutional and Quality Improvement			
4.2.2.09 Control: Documented procedures exist for incident analysis.	❒	❒	
4.2.2.10 Quality: Personnel are aware of, knowledgeable of, and consistently follow or use the procedures, technologies, and methodologies used to perform this task.	❒	❒	
4.2.2.11 Quality: A process and criteria exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	
4.2.2.12 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	Met (all Required indicators have Yes answers)	❒	Not Met (one or more Required indicators have a No answer)	❒
Not Applicable		❒	Not Observed	❒

Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement

- Record information and analysis in a tracking system or database to help correlate and search for related events, intruder modus operandi (MO), exploits, and countermeasures.
- Use criteria (such as consistency, clarity, usefulness, applicability, and meaningfulness) for evaluating how well this activity is performed and the quality of its artifacts.

4.2 ANALYSIS

4.2.3 Incident correlation is performed to identify similar activity. **Priority II**

Clarification

This capability focuses on correlating activity across incidents to determine any interrelations, patterns, common intruder signatures, common targets, or exploitation of common vulnerabilities. Incident correlation

- broadens the view of the nature, scope, and impact of malicious activity
- identifies relationships and interdependencies that can help develop and implement comprehensive solutions

Types of information that can be correlated include

- IP addresses, hostnames, ports, protocols, and services
- targeted applications, OSs, organizational sectors, site names, and business functions
- common attacks and exploits

Incident correlation can identify where activity is more widespread than originally thought and identify any relationships among malicious attacks, compromises, and exploited vulnerabilities. Often incidents are reported individually, correlation allows analysts to see that a particular malware may have affected multiple systems on their organizational infrastructure instead of just one. It may also point to a specific type of employee role which might be targeted with a phishing attack.

Incident correlation can be used to pull information from multiple logs or data sources within an organization to corroborate and substantiate malicious activity.

Incident correlation is not fusion analysis. Fusion analysis is its own capability and looks at pulling together disparate data sources to bring a broader picture to the incident context. Incident correlation looks across incidents reported within the organization for common activity or targets. In some cases information can be correlated that comes from outside the organization, this will show that the activity at the organization is part of a broader attack across the internet community.

Team Guidance

The team should look for evidence that the

- IM function understands the requirements and methodologies for performing incident correlation
- analysis is performed in a consistent, accurate, timely, and complete manner
- the appropriate correlation tools are in place and understood by the incident analysts

The IM function should be able to show some examples of interrelationships between incidents. In some cases, the IM function may also rely on incident correlation performed by others and should be able to demonstrate how they collect and use that information. The team does not have to have all possible data sources, but more is better.

The team could have the incident management personnel walk through how they perform correlation, showing what tools they use and what analysis is done.

References

Regulatory References: None

Guidance References: None

[indirect]

NIST SP 800-61 Rev 2 *Computer Security Incident Handling Guide* [Cichonski 2012]

> "Sec 3.2.3 Sources of Precursors and Indications
>
> Precursors and indications are identified using many different sources, with the most common being computer security software alerts, logs, publicly available information, and people.
>
> Sec 3.2.4 Incident Analysis
> Perform Event Correlation. Evidence of an incident may be captured in several logs. […] Correlating events among multiple indication sources can be invaluable in validating whether a particular incident occurred, as well as rapidly consolidating the pieces of data."

NIST SP 800-92 *Guide to Computer Security Log Management* [Kent 2006a]

> "Sec 3.2 Functions
> [p 3-4] "Analysis
> – *Event correlation* is finding relationships between two or more log entries. The most common form of event correlation is rule-based correlation, which matches multiple log entries from a single source or multiple sources based on logged values, such as timestamps, IP addresses, and event types."

Organization Response

Examples of Evidence Sought

- ❑ Sample outputs of correlation activities
- ❑ Sample recommendations for remediation or countermeasures based on correlation
- ❑ Observation or demonstration of correlation analysis tools and methodologies
- ❑ Observation or demonstration of incident tracking system or database showing any evidence of correlation
- ❑ Observation of personnel performing incident correlation

Scoring Criteria	Yes	No	Evidence
Required			
4.2.3.01 Control: A correlation process exists.	❒	❒	
4.2.3.02 Control: Personnel are trained appropriately on the relevant process, technology, and methodologies for performing this type of analysis.	❒	❒	

4.2.3.03 Activity: Incident correlation is conducted.	❒	❒	
4.2.3.04 Activity: Recommendations are developed, as appropriate, based on correlation analysis.	❒	❒	
4.2.3.05 Activity: Incident correlation results are provided to the appropriate technical and management personnel.	❒	❒	
4.2.3.06 Activity: Sanitized information is provided to other organizations if applicable according to organizational guidelines.	❒	❒	
Recommended Best Practices			
4.2.3.07 Activity: Personnel know how to obtain and use analysis reports provided by other organizations or vendors.	❒	❒	
4.2.3.08 Activity: Security incident and event management (SIEM) tools are installed and used for correlation by the incident management personnel.	❒	❒	
4.2.3.09 Quality: Automated correlation tools are built into any incident tracking or logging system.	❒	❒	
Institutional and Quality Improvement			
4.2.3.10 Control: Documented procedures exist for correlation.	❒	❒	
4.2.3.11 Quality: Personnel are aware of, knowledgeable of, and consistently follow or use the procedures, technologies, and methodologies used to perform this task.	❒	❒	
4.2.3.12 Quality: A process and criteria exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	
4.2.3.13 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒
Not Applicable		❒	**Not Observed**	❒

Evidence Collected					
Document Review		Interviews		Direct Observation	
Notes					
Suggestions for Improvement					
None					

4.2 ANALYSIS

4.2.4 Impact of an incident is determined. **Priority II**

Clarification

This capability assesses whether the impact of an incident is determined during the incident analysis process. Without information about how an incident has affected an organization, incident responders cannot accurately plan containment, remediation, or eradication efforts.

The purpose of impact analysis is to determine the breadth and severity of an incident to facilitate additional steps in the incident response process. Incident management personnel may use the results of impact analysis to further prioritize cases during and after the triage process.

Team Guidance

Assessment teams should look for evidence of impact analysis as part of the incident analysis processes. Note that impact analysis may be an insufficiently described part of incident analysis processes that are already documented.

Impact analyses should identify how specific incident may affect or are affecting an organization. A lack of impact analysis procedure can be apparent when incidents are described without referencing the effects the incident has on an organization's systems, software, or information.

References

Regulatory References: None

Guidance References:

NIST SP 800-30 Rev 2 *Guide for Conducting Risk Assessment* [2012]

> Chapter 2, Impact
>
> The level of impact from a threat event is the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability. […]
>
> Charter 3, Determine Impact
>
> Determine the adverse impacts from threat events of concern considering: (i) the characteristics of the threat sources that could initiate the events; (ii) the vulnerabilities/ predisposing conditions identified; and (iii) the susceptibility reflecting the safeguards/countermeasures planned or implemented to impede such events. […]

Organization Response

Examples of Evidence Sought			
❑ Sample of system, software, or information inventory for the assessed organization ❑ Records of incident analyses containing impact assessments ❑ Standardized forms or categories for recording and assessing impact ❑ Inventory records indicating currently maintained systems, software, and information			
Scoring Criteria	Yes	No	Evidence
Required			
4.2.4.01 Activity: Impact to the function of systems, software, and critical processes are assessed in the course of incident analysis.	❒	❒	
4.2.4.02 Activity: Impact to organizational information is assessed in the course of incident analysis.	❒	❒	
Recommended Best Practices			
4.2.4.03 Control: Accurate inventories of an organization's systems and their organizational importance are available.	❒	❒	
4.2.4.04 Control: Accurate inventories of an organization's software and their organizational importance are available.	❒	❒	
4.2.4.05 Control: Accurate inventories of an organization's configuration standards are available.	❒	❒	
4.2.4.06 Control: Accurate lists of an organization's critical processes are available.	❒	❒	
4.2.4.07 Prerequisite: There are predefined categories of incident impact.	❒	❒	
Institutional and Quality Improvement			
4.2.4.08 Control: Documented procedures exist for assessing and categorizing incident impacts.	❒	❒	
4.2.4.09 Quality: A process exists for re-evaluation and alteration of the impact analysis process.	❒	❒	

Scoring	**Met (all Required**	❒	**Not Met (one or more Required indicators have a No answer)**	❒

	indicators have Yes answers)				
Not Applicable		❒	**Not Observed**		❒
Evidence Collected					
Document Review		Interviews		Direct Observation	
Notes					
Suggestions for Improvement					
• Accurately track your inventory of systems, software, and information in order to properly assess the impact of an incident. • Conduct a clearly defined impact assessment as part of the incident analysis process.					

4.2 ANALYSIS

4.2.5 Incident root cause analysis is conducted. Priority II

Clarification

This capability focuses on whether the CSIRT analyzes all available information, supporting evidence, and artifacts related to a computer security event or incident to determine the underlying root cause of an incident.

Root cause analysis is a specific subset of incident analysis, typically focusing on "the understanding of the *design* or *implementation* flaw that allowed the attack."[22] Understanding the root cause of an incident can support the development of an appropriate, more focused and targeted response or course of actions. In addition, root cause identification can help to develop indicators/signatures to better prevent or detect future incidents.

Depending on the circumstances, mitigation (elimination of the root cause) and recovery might not happen in the short term; some post-analysis response actions may be deferred until a later time.

Root cause analysis differs from other types of analysis, such as impact analysis.

Root cause analysis may require the results or information from other types of analysis, such as

- system analysis
- network analysis
- malware analysis
- vulnerability analysis
- retrospective analysist (what else did the attacker do?)
- trend analysis

Team Guidance

The team should determine that the CSIRT uses a methodical approach for analyzing the available information to identify the suspected root cause or threat vectors. This requires

- a list, catalog, or taxonomy of possible causes or threat vectors
- information sources to identify (confirm or refute) the possible threat vectors
- a methodical approach (defined processes) for analyzing the available information to identify the suspected threat vectors

Note that, with the exception of the additional above requirements (controls), the indicators in this capability are similar to (mirror) the indicators for the general incident analysis capability (4.2.2); the indicators in this capability are specifically focused on root cause analysis.

[22] Definition from FIRST "CSIRT Services Framework"

References

Regulatory References: None

Guidance References:

[indirect]

SP 800 NIST-61 Rev 2 *Computer Security Incident Handling Guide* [Cichonski 2012]

> "Sec 3.2.4 Incident Analysis
>
> […]
>
> Incident handlers are responsible for analyzing ambiguous, contradictory, and incomplete symptoms to determine what has happened. […]
>
> The incident response team should work quickly to analyze and validate each incident, following a pre-defined process and documenting each step taken. When the team believes that an incident has occurred, the team should rapidly perform an initial analysis to determine the incident's scope, such as which networks, systems, or applications are affected; who or what originated the incident; and how the incident is occurring (e.g., what tools or attack methods are being used, what vulnerabilities are being exploited). The initial analysis should provide enough information for the team to prioritize subsequent activities, such as containment of the incident and deeper analysis of the effects of the incident.
>
> **Seek Assistance from Others**. […] It is important to accurately determine the cause of each incident so that it can be fully contained and the exploited vulnerabilities can be mitigated to prevent similar incidents from occurring."

NIST SP 800-53 Rev. 4 *Security and Privacy Controls for Federal Information Systems and Organizations* [NIST 2013]

> "IR-4 INCIDENT HANDLING
>
> **Control:** The organization:
>
> (c.) Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;"

A Step-by-Step Approach on How to Set Up A CSIRT [ENISA, 2006]

> "A.2 CSIRT Services
>
> Incident analysis
>
> There are many levels of incident analysis and many sub-services. Essentially, incident analysis is an examination of all available information and supporting evidence or artifacts related to an incident or event. The purpose of the analysis is to identify the scope of the incident, the extent of damage caused by the incident, the nature of the incident, and available response strategies or workarounds. The CSIRT may use the results of vulnerability and artifact analysis (described below) to understand and provide the most complete and up-to-date analysis of what has happened on a specific system."

Organization Response

Examples of Evidence Sought

- ❑ Documented processes for conducting root cause analysis

- ❑ Sample root cause analysis findings included within the incident tracking system or as stand-alone reports
- ❑ Sample recommendations for remediation or countermeasures
- ❑ Observation or demonstration of tools supporting root cause analysis
- ❑ Observation or demonstration of incident tracking systems containing root cause analysis results

Scoring Criteria	Yes	No	Evidence
Required			
4.2.5.01 Control: A list, catalog, or taxonomy of possible causes or threat vectors exists.	❒	❒	
4.2.5.02 Control: Information sources are available/accessible to identify (confirm or refute) the possible threat vectors.	❒	❒	
4.2.5.03 Control: An incident root cause analysis process exists.	❒	❒	
4.2.5.04 Control: Personnel are appropriately trained on the relevant process, technology, and methodologies.	❒	❒	
4.2.5.05 Activity: Personnel conduct a level and type of root cause analysis appropriate to the incident's category and severity.	❒	❒	
4.2.5.06 Activity: Root cause analysis of an incident is performed.	❒	❒	
4.2.5.07 Activity: Incident root cause analysis reports are generated according to the process and then archived.	❒	❒	
4.2.5.08 Activity: Root cause analysis output is used to provide recommendations or countermeasures to mitigate the incident.	❒	❒	
Recommended Best Practices			
4.2.5.09 Activity: Incident root cause analysis reports are provided to the affected constituents according to organizational guidelines.	❒	❒	
4.2.5.10 Activity: Sanitized information is provided to other constituents or external contacts as appropriate.	❒	❒	

Institutional and Quality Improvement			
4.2.5.11 Control: Documented procedures exist for incident root cause analysis.	❒	❒	
4.2.5.12 Quality: Personnel are aware of, knowledgeable of, and consistently follow or use the procedures, technologies, and methodologies used to perform this task.	❒	❒	
4.2.5.13 Quality: A process and criteria exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	
4.2.5.14 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒
Not Applicable		❒	**Not Observed**	❒

Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement

- Record information and root cause analysis results in a tracking system or database to help identify intruder modus operandi (MO), vulnerabilities, exploits, and countermeasures.
- Use criteria (such as clarity, usefulness, applicability, and meaningfulness) for evaluating how well this activity is performed and the quality of its artifacts.

4.2 ANALYSIS

4.2.6 Fusion analysis is performed to identify concerted attacks and shared vulnerabilities.

Priority III

Clarification

Fusion analysis is the analysis of data from disparate sources to determine connections between attacks, vulnerabilities, threats, and weaknesses. Because attacks and other malicious activity rarely occur in isolation, an organization must analyze data from disparate sources to identify their true scope, impact, and risk. The resulting "big picture" view helps the organization understand the relationship between ongoing incidents or potential threats, and identify effective countermeasures and remediation strategies. That understanding can lead to a more widespread solution to computer security problems. It also allows the organization to develop more targeted and comprehensive recommendations and countermeasures.

When conducting fusion analysis, organizations often analyze data from these sources: research on well-known attacks; incident reports; vulnerability exposures; network traffic; system and network configurations and environments; media reports; and other situational awareness data. Looking at such varied sources helps organizations recognize a concerted attack signature, identify common widespread vulnerabilities, and predict the potential victims of targeted attacks. The organization can also use this information to gain a better understanding of the full scope and impact of malicious activity and any related vulnerabilities.

Fusion analysis tools may include the ability to provide visualizations or a common operating picture (COP) that can integrate and display information from multiple sources in a readily-understandable format.[23] The use of a COP or other visualization tools in fusion analysis can help the organization to achieve better situational awareness.

Note that this is a higher level form of research that requires specific expertise and access to multiple data sources. Some organizations may lack the expertise or tools needed to perform it. Organizations that don't do such analysis may have a limited understanding of the ongoing risks and threats and, as a result, develop ineffective countermeasures and recommendations.

Based on the results of that analysis, additional research can be done to determine which patterns of attacks are emerging and which security problems must be addressed. Using this information, organizations can determine effective resolution and mitigation strategies, and where they must be applied.

[23] An example of this is the DHS Analysis and Operations COP program:
"The Common Operational Picture (COP) is the core DHS situational awareness (SA) capability for effective decision making, rapid staff actions, and appropriate mission execution. It is an integrated SA application that supports the DHS mission of responding to threats and hazards to the nation by collecting, sharing and displaying multi-dimensional information that facilitates collaborative planning, and responses to these threats. […] In FY09, DHS identified three key technology enhancement to be integrated into A&O COP program: 1) improving NOC Senior Watch Officer (SWO) data infusion; 2) auto-ingestion of data from multiple sources; and 3) creation of a consolidated, centralized data repository. The benefits of these enhancements are real-time, situational awareness, alerts, advanced analytics, data visualization, and collaboration with the DHS Geospatial Information Infrastructure."
(Source: *IT Program Assessment: DHS A&O COP* [DHS 2012b])

Team Guidance

The assessment team should determine that the IM function understands the requirements and methods for fusion analysis and that the analysis is performed in a consistent, accurate, timely, and complete manner. The team should ensure that a variety of data sources are used to provide a comprehensive view of threats and risks.

References

Regulatory References: None

Guidance References: None

[indirect]

NIST SP 800-61 Rev 2 *Computer Security Incident Handling Guide* [Cichonski 2012]

> "Sec 3.2.3 Sources of Precursors and Indications
> Precursors and indications are identified using many different sources, with the most common being computer security software alerts, logs, publicly available information, and people.
>
> Sec 3.2.4 Incident Analysis
> Perform Event Correlation. Evidence of an incident may be captured in several logs. […] Correlating events among multiple indication sources can be invaluable in validating whether a particular incident occurred, as well as rapidly consolidating the pieces of data."

Organization Response

Examples of Evidence Sought

- ❑ Samples of data sources used (incident reports, vulnerability reports, system and network configurations, network traffic logs, current events and news feeds, etc.)
- ❑ Sample fusion analysis reports identifying common problems, related attacks, and shared vulnerabilities
- ❑ Sample recommendations for prevention strategies, remediations, or countermeasures
- ❑ Observation or demonstration of tools supporting fusion analysis
- ❑ Observation of personnel performing fusion analysis

Scoring Criteria	Yes	No	Evidence
Required			
4.2.6.01 Prerequisite: Various sources of data, incidents, and vulnerabilities are available and accessible.	❒	❒	
4.2.6.02 Control: A fusion analysis process exists.	❒	❒	
4.2.6.03 Control: Personnel are appropriately trained on the relevant process, technology, and methodologies.	❒	❒	

4.2.6.04 Activity: Data from disparate sources is routinely synthesized to determine connections between events, incidents, vulnerabilities, and activities ongoing in or external to the organization.	❒	❒	
4.2.6.05 Activity: Fusion analysis reports are generated according to the process and then archived.	❒	❒	
4.2.6.06 Activity: Fusion analysis reports are provided to the appropriate technical and management personnel according to organizational guidelines.	❒	❒	
4.2.6.07 Activity: Sanitized information is provided to other external contacts and organizations according to organizational guidelines.	❒	❒	
4.2.6.08 Activity: Retrospective analysis findings have recommendations and countermeasures to address the incident.	❒	❒	
Recommended Best Practices			
4.2.6.09 Control: Fusion analysis tools provide visualization or common operational picture features to enhance situational awareness.	❒	❒	
Institutional and Quality Improvement			
4.2.6.10 Control: Documented procedures exist for fusion analysis.	❒	❒	
4.2.6.11 Quality: Personnel are aware of, knowledgeable of, and consistently follow or use the procedures, technologies, and methodologies used to perform this task.	❒	❒	
4.2.6.12 Quality: A process and criteria exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	
4.2.6.13 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒
Not Applicable		❒	**Not Observed**	❒

Evidence Collected					
Document Review		Interviews		Direct Observation	
Notes					
Suggestions for Improvement					
• Use criteria (such as timeliness, completeness, clarity, usefulness, applicability, and accuracy) for evaluating how well this activity is performed and the quality of its artifacts.					

4.2 ANALYSIS

4.2.7 Retrospective analysis is conducted. Priority III

Clarification

This capability focuses on whether information and reports are routinely analyzed from a historical perspective to provide both a broad view of emerging threats and risks, and an assessment of the success of resolution strategies. Retrospective analysis identifies

- ineffective resolutions that require new solutions
- emerging problem areas that require attention

This analysis can confirm positive actions that have strengthened the organization's ability to correct security problems. Retrospective analysis can look at the actions that have been taken to manage incidents, attacks, and vulnerabilities over time, and then compare them to the current state to determine if those actions had positive long-term effects or successful outcomes (i.e., those problems are not recurring and were mitigated successfully). Such analysis requires looking at response times and strategies, and changes in reports over time and in the organization's security posture. The types of incidents, vulnerabilities, and attacks that have been seen over time are also reviewed. In this case, the analysis is used to help identify high-risk areas, continuing and high-volume incidents, and both emerging and ongoing problem areas.

Note that conducting this retrospective analysis is broader (typically looking across many incidents) and more long-term than the postmortem reviews that may be held after individual, significant incidents (see capability 4.3.6).

Team Guidance

The team should look for evidence that the IM function not only understands the requirements and methodologies for performing retrospective analysis, but also performs the analysis in a consistent, accurate, timely, and complete manner. Evidence should show that the organization analyzes historical data to determine how effective resolution strategies have been and to identify areas for further improvement.

Note that this is higher level analysis, requiring access to historical data about incidents, attacks, vulnerabilities, actions taken, and changes in the infrastructure or environment. Not all organizations may have the expertise, historical data, or time necessary to perform such analysis. Whether this capability will be included should be determined during the assessment scoping. If it is not within the scope, the capability should be marked as not applicable.

References

Regulatory References: None

Guidance References:

[indirect]

NIST SP 800-61 Rev 2 *Computer Security Incident Handling Guide* [Cichonski 2012]

"Sec 3.4.2 Using Collected Incident Data
[p 3-25]

Lessons learned activities should produce a set of objective and subjective data regarding each incident. Over time, the collected incident data should be useful in several capacities. […] A study of incident characteristics may indicate systemic security weaknesses and threats, as well as changes in incident trends. This data can be put back into the risk assessment process, ultimately leading to the selection and implementation of additional controls. Another good use of the data is measuring the success of the incident response team. If incident data is collected and stored properly, it should provide several measures of the success (or at least the activities) of the incident response team. […]"

NIST SP 800-53 Rev. 4 *Security and Privacy Controls for Federal Information Systems and Organizations* [NIST 2013]

"RA-5 VULNERABILITY SCANNING

Control Enhancements:

(8.) The organization reviews historic audit logs to determine if a vulnerability identified in the information system has been previously exploited."

Good Practice Guide for Incident Management [ENISA, 2010]

"8.6.1 Proposals for improvement
Incident handling is, of course, a reactive service. It can be a first step to providing proactive actions for the improvement of security awareness. You can learn much from incidents you handled but you can also teach others a lot Who can benefit from this? Use the same set of parties with whom you collaborated or contacted during the resolution of an incident (see section 8.4 Incident resolution). Try to take advantage of what you have learnt from incidents that came to your team for resolution. This is usually very valuable material that can be used effectively in your awareness building activities. […]"

Organization Response

Examples of Evidence Sought

- ❑ Samples of data sources used (e.g., incident reports, vulnerability reports, network traffic analysis, reports on response actions or countermeasures taken over the years)
- ❑ Sample retrospective analysis reports
- ❑ Observation or demonstration of tools supporting retrospective analysis

Scoring Criteria	Yes	No	Evidence
Required			
4.2.7.01 Prerequisite: Historical data on incidents, vulnerabilities, and applied remediations or countermeasures is available to and accessible by incident management personnel.	❒	❒	
4.2.7.02 Control: A process exists for retrospective analysis.	❒	❒	
4.2.7.03 Control: Personnel are appropriately trained on the relevant process, technology, and methodologies.	❒	❒	

4.2.7.04 Activity: Historical data and information related to incidents, attacks, vulnerabilities, and applied countermeasures are reviewed at least annually to determine the long-term effects, outcomes, effectiveness, emerging problems, and trends.	❒	❒	
4.2.7.05 Activity: Retrospective analysis reports are generated according to the process and then archived.	❒	❒	
4.2.7.06 Activity: Retrospective analysis reports are provided to the appropriate technical and management personnel according to organizational guidelines.	❒	❒	
4.2.7.07 Activity: Sanitized information is provided to other organizational components and external contacts according to organizational guidelines.	❒	❒	
4.2.7.08 Activity: Analysis findings where security posture is still at risk are addressed.	❒	❒	
Recommended Best Practices			
None	❒	❒	
Institutional and Quality Improvement			
4.2.7.09 Control: Documented procedures exist for retrospective analysis.	❒	❒	
4.2.7.10 Quality: Personnel are aware of, knowledgeable of, and consistently follow or use the procedures, technologies, and methods used to perform this task.	❒	❒	
4.2.7.11 Quality: A process and criteria exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	
4.2.7.12 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒
Not Applicable		❒	**Not Observed**	❒

Evidence Collected					
Document Review		Interviews		Direct Observation	
Notes					
Suggestions for Improvement					
• Use criteria (such as timeliness, completeness, and accuracy) for evaluating how well this activity is performed and the quality of its artifacts.					

4.2 ANALYSIS

4.2.8 Media analysis is performed on constituent networks and systems. Priority II

Clarification

This capability focuses on whether the organization has the ability to perform (when required) the collection, preservation, documentation, and analysis of evidence from a compromised computer system[24] to identify changes to the system and help reconstruct the events that led to the compromise. Note that because this is a very specialized form of analysis that requires special tools, training, skills, and processes, as well as the ability to access constituents' networks and systems (and perhaps travel to the constituent's site, if needed),some organizations may not be able to perform it. Therefore, sometimes this capability may be performed by an internal or external forensics team or LE.

If performed for forensic purposes, the gathering of information and evidence must be done in a way that documents a provable chain of custody that is admissible in a court of law under the rules of evidence.

Media or forensic analysis can be used to determine the extent to which a system or network has been compromised or otherwise affected. This results in a better understanding of what malicious activity occurred and what other systems or services may have been affected. Such analysis can also facilitate the development and implementation of comprehensive solutions, ensuring the use of more effective protective strategies. The results of media analysis can also be used to prosecute malicious intruders.

Policies, procedures, and training are needed to ensure personnel performing this analysis do not damage or invalidate forensic evidence. These efforts include outlining how and when LE is involved in the analysis. In addition, personnel performing this function for forensic purposes may need to be prepared to act as expert witnesses in court proceedings if the evidence analyzed is used in a court of law to prosecute the intruder.

Team Guidance

Note that for this capability "media analysis" means analysis of any media, even non-digital that may provide information that can be used to understand what malicious activity has occurred.

The team should verify that the IM function understands digital media (and forensic, if provided) analysis requirements and methodologies, and performs the analysis in a consistent, accurate, timely, secure, and complete manner. Forensic analysis must follow the chain of custody rules. The organization should be able to analyze systems and networks to determine the exact changes that have been made and should be able to document the analysis according to the rules of evidence.

Often, this capability is performed by a specialized group within or external to the organization. If done by an internal group, assess it for its capability. If done by an external group, determine if that information is appropriately passed to that external group and results are returned to the organization per organizational guidelines, the SLA, or other requirements.

---

[24] As in NIST SP 800-86, the term *computer* in this capability is used to refer to all computing, storage, and peripheral devices (including networking equipment, printers, removable media, cell phones, etc.).

References

Regulatory References: None

Guidance References:

NIST SP 800-61 Rev 2 *Computer Security Incident Handling Guide* [Cichonski 2012]

> "Sec. 3.3.2 Evidence Gathering and Handling
> [p 36]
>
> Although the primary reason for gathering evidence during an incident is to resolve the incident, it may also be needed for legal proceedings. In such cases, it is important to clearly document how all evidence, including compromised systems, has been preserved. Evidence should be collected according to procedures that meet all applicable laws and regulations that have been developed from previous discussions with legal staff and appropriate law enforcement agencies so that any evidence can be admissible in court. In addition, evidence should be accounted for at all times; whenever evidence is transferred from person to person, chain of custody forms should detail the transfer and include each party's signature. A detailed log should be kept for all evidence […]
>
> Sec 3.4.3 Evidence Retention
> [p 41]
>
> Prosecution. If it is possible that the attacker will be prosecuted, evidence may need to be retained until all legal actions have been completed. In some cases, this may take several years. Furthermore, evidence that seems insignificant now may become more important in the future. […]
>
> Data Retention.
> Most organizations have data retention policies that state how long certain types of data may be kept. […] GRS 24 specifies that incident handling records should be kept for three years."

NIST SP 800-86 *Guide to Integrating Forensic Techniques into Incident Response* [Kent 2006b]

> "Sec 1.2 Purpose and Scope
> [p 1-1]
>
> This publication is intended to help organizations in investigating computer security incidents and troubleshooting some information technology (IT) operational problems by providing practical guidance on performing computer and network forensics.
>
> Sec 2.6 Recommendations
> [p 2-8]
>
> The key recommendations on establishing and organizing a forensic capability are as follows:
>
> - Organizations should have a capability to perform computer and network forensics.
> - Organizations should determine which parties should handle each aspect of forensics.
> - Incident handling teams should have robust forensic capabilities.
> - Many teams within an organization should participate in forensics.
> - Forensic considerations should be clearly addressed in policies.
> - Organizations should create and maintain guidelines and procedures for performing forensic tasks."

A Step-by-Step Approach on How to Set Up A CSIRT [ENISA, 2006]

> "A.2 CSIRT Services
> Incident Analysis…
> Forensic evidence collection
> The collection, preservation, documentation, and analysis of evidence from a compromised

computer system to determine changes to the system and to assist in the reconstruction of events leading to the compromise. This gathering of information and evidence must be done in a way that documents a provable chain of custody that is admissible in a court of law under the rules of evidence. Tasks involved in forensic evidence collection include (but are not limited to) making a bit-image copy of the affected system's hard drive; checking for changes to the system such as new programs, files, services, and users; looking at running processes and open ports; and checking for Trojan horse programs and toolkits. CSIRT staff performing this function may also have to be prepared to act as expert witnesses in court proceedings."

Organization Response

Examples of Evidence Sought

- ❑ Results or reports from media investigations and analysis
- ❑ Documentation showing chain of custody is followed
- ❑ Sample recommendations for remediation or countermeasures based on media analysis
- ❑ Toolkit of system examination programs, file integrity checkers, and so forth
- ❑ Safes and other secure storage areas used for evidence
- ❑ Media analysis tools and methodologies
- ❑ Evidence collection tools[25] and methodologies
- ❑ Observation of personnel performing media analysis

Scoring Criteria	Yes	No	Evidence
Required			
4.2.8.01 Control: Criteria are defined for when media analysis should be conducted on incidents.	❒	❒	
4.2.8.02 Control: A process exists for performing media analysis.	❒	❒	
4.2.8.03 Control: Personnel are appropriately trained on the relevant processes, technologies, and methodologies needed to conduct media analysis.	❒	❒	
4.2.8.04 Activity: Forensic evidence is collected and analyzed according to evidence handling rules.	❒	❒	
4.2.8.05 Activity: Media analysis results and reports are generated according to the process and then archived.	❒	❒	

[25] Per NIST SP 800-61 Rev 2 [p 22], evidence-gathering accessories include "hard-bound notebooks, digital cameras, audio recorders, chain of custody forms, evidence storage bags and tags, and evidence tape, to preserve evidence for possible legal actions."

4.2.8.06 Activity: Media analysis results and reports are provided to the appropriate technical, management, and legal personnel according to organizational guidelines.	❒	❒	
4.2.8.07 Activity: Forensic evidence and analysis results and reports are passed to LE for prosecution when appropriate and approved by management and/or Legal.	❒	❒	
Recommended Best Practices			
4.2.8.08 Control: Criteria are defined for when and how LE should be contacted.	❒	❒	
4.2.8.09 Control: A POC within the organization has been identified to work with LE.	❒	❒	
4.2.8.10 Control: First responder guidelines exist and are published to incident handlers and systems administrators in the organizational divisions and branches.	❒	❒	
Institutional and Quality Improvement			
4.2.8.11 Control: Documented procedures exist for media analysis.	❒	❒	
4.2.8.12 Control: Documented procedures exist for following chain of custody and rules of evidence.	❒	❒	
4.2.8.13 Quality: Personnel are aware of, knowledgeable of, and consistently follow or use the procedures, technologies, and methodologies used to perform this task.	❒	❒	
4.2.8.14 Quality: A process and criteria exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	
4.2.8.15 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒
Not Applicable		❒	**Not Observed**	❒

Evidence Collected					
Document Review		Interviews		Direct Observation	
Notes					
Suggestions for Improvement					
• Use criteria (such as completeness, accuracy, clarity, usefulness, and adherence to defined levels of risk/threat/impact) to evaluate how well this activity is performed and the quality of its artifacts.					

4.2 ANALYSIS

4.2.9 Artifact or malware analysis is conducted.

Priority II

Clarification

This capability involves activities related to understanding the capabilities and intent of artifacts (e.g., malware, exploits, spam, and configuration files) and their delivery, detection, and neutralization.

As part of the incident handling process, digital artifacts may be found on affected systems or malware distribution sites. Artifacts may be the remnants of an intruder attack, such as scripts, files, images, configuration files, tools, tool outputs, logs, etc.

Artifact analysis is done to find out how the artifact may have been used by an intruder, such as to get into an organization's systems and networks, or to identify what the intruder did once in the system. Artifact analysis strives to identify how the artifact operates on its own or in conjunction with other artifacts. This can be achieved through various types of activities including: surface analysis, reverse engineering, runtime analysis, and comparative analysis. Each activity provides more information about the artifact. Analysis methods include but are not limited to identification of type and characteristics of artifact, comparison to known artifacts, observation of artifact execution in a runtime environment, and disassembling and interpreting binary artifacts.

By doing an analysis of the artifact(s), an analyst tries to reconstruct and determine what the intruder did, in order to assess damage, develop solutions to mitigate against the artifact, and provide information to constituents and other researchers.

If the organization cannot perform this activity itself, it should have access to other entities either through contractors or coordination centers or law enforcement that can perform this analysis task if needed.

An artifact or malware analysis capability includes

- establishing an appropriate test facility or lab to conduct the analysis that protects production systems from infection
- establishing policies and procedures and guidance for performing artifact and malware analysis
- monitoring anti-malware sites and organizations to gather intelligence on new attack vectors and techniques
- alerting the constituent to potential or current malware threats and corresponding remediation guidance based on the analysis
- keeping up to date on new developments in malware through research, training, mentoring, and other professional development efforts
- coordinating with other internal and external parties, such as organizational IT experts, vendors, other CSIRTs, ISPs, AV groups, and other security experts, to prevent or mitigate threats and malicious activity

Collaboration and coordination of artifact or malware analysis requires defined processes, roles, and responsibilities both internally and externally.

Team Guidance

If the organization does not perform this activity itself, but has another group that performs the task for it, this capability should be addressed to that entity. If it can be substantiated that the other entity performs this capability according to the indicators then that should be counted as the organization meeting the capability.

References

Regulatory References: None

Guidance References: None

Organization Response

Examples of Evidence Sought

- ❑ Observation of incident management personnel performing artifact or malware analysis
- ❑ Copies of recent artifact or malware analysis results or reports
- ❑ Observation or demonstration of a malware analysis repository or catalog
- ❑ Recent email or web malware warnings and advisories sent to constituents
- ❑ Recent sharing of indicators of compromise with constituents
- ❑ Website (or other mechanism) for posting anti-malware signatures for constituents to download
- ❑ Copies of procedures or guidance for performing artifact or malware analysis
- ❑ Observation of test or lab facility for artifact and malware analysis
- ❑ Observation of incident management personnel developing signatures based on analysis

Scoring Criteria	Yes	No	Evidence
Required			
4.2.9.01 Control: Incident management personnel are appropriately trained on the process and technologies used to conduct artifact or malware analysis.	❒	❒	
4.2.9.02 Activity: Available, approved artifact analysis tools are used in accordance with organizational requirements.	❒	❒	
4.2.9.03 Activity: Sources of information on emerging malware (e.g., FIRST, vendor AV sites, and other similar organizations) are reviewed.	❒	❒	
4.2.9.04 Activity: Artifact or malware analysis is conducted.	❒	❒	

4.2.9.05 Activity: The nature of a recovered digital artifact along with its relationship to other artifacts, attacks, and exploited vulnerabilities is determined during analysis as possible.	❒	❒	
4.2.9.06 Activity: Constituents are alerted to emerging or current malware threats per SLA or organizational requirements.	❒	❒	
4.2.9.07 Activity: Signatures for new malware found are created and shared with approved stakeholders, partners, and constituents.	❒	❒	
4.2.9.08 Activity: A current list of POCs for malware notifications and alerts is maintained.	❒	❒	
4.2.9.09 Activity: If organization does not perform artifact or malware analysis they have a relationship in place to pass on malware for analysis.	❒	❒	
Recommended Best Practices			
4.2.9.10 Activity: A repository or catalog of analyzed malware is maintained.	❒	❒	
Institutional and Quality Improvement			
4.2.9.11 Control: Documented procedures exist that describe the process and method used (including notifications, alerts, and remediation assistance) to provide this task.	❒	❒	
4.2.9.12 Quality: Personnel are aware of, knowledgeable of, and consistently perform or use the procedures, processes, methodologies, and technologies for performing this task.	❒	❒	
4.2.9.13 Quality: A process and criteria exist for evaluating how well this activity is performed and the quality of its outputs.	❒	❒	
4.2.9.14 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒

Not Applicable	❒	Not Observed	❒

Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement

- Monitor AV and alert websites and mailing lists daily.
- Define document types and create corresponding templates for disseminating information.
- Improve malware analysis techniques, build a test environment or lab facility, and add automated tools for collecting information on malware.
- Develop technical relationships with trusted experts (e.g., product vendors, anti-virus vendors, coordination centers, and other CSIRTs).
- Keep POC lists up to date, reviewing them at least monthly.

4.3 INCIDENT RESPONSE

4.3.1 General incident response guidance and procedures are distributed to constituents.

Priority II

Clarification

The constituency may not be as knowledgeable as incident management personnel on the best methods for testing and installing patches, changing configurations, and implementing workarounds and other mitigation strategies.

The focus of this capability is to ensure that constituents are provided with general guidance for how to respond to identified incidents. This guidance will usually come from the incident management function, since that is the group that provides response and mitigation recommendations. The purpose of the guidance is to provide constituents with a basic process for handling mitigation and resolution recommendations in a consistent and standardized way. The general guidance is basically direction or instruction for local response at the business unit level. This is different than providing guidance for a particular incident resolution (which is covered in 4.3.2). In the case of a specific incident, the recommendations relate to technical advice for performing a response to that incident. The general guidance discussed in this capability is more process focused, providing some context for handling any incident that occurs.

The general guidance can take the form of guidelines, checklists, training, or other materials, as appropriate. The guidance can be organization-specific and developed by incident management personnel, or can be adapted from provided Federal or third-party materials. If adapted from other materials, incident management personnel should always review them for relevance and applicability to the constituency.

Team Guidance

The team should look for evidence to show that up-to-date guidance is built, acquired, maintained, and routinely distributed to the organization.

This particular activity may not be applicable if, for example, a formal CSIRT performs all the response activities. If this capability is deemed not applicable, the rationale should be documented, and the team should judge whether the rationale is sufficient.

References

Regulatory References: None

Guidance References: None

[indirect]

NIST SP 800-53 Rev. 4 *Security and Privacy Controls for Federal Information Systems and Organizations* [NIST 2013]

7. “IR-7 INCIDENT RESPONSE ASSISTANCE

   Control: The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

Supplemental Guidance: Incident response support resources provided by organizations include, for example, help desks, assistance groups, and access to forensics services, when required."

Organization Response

Examples of Evidence Sought

- ❑ Sample procedures, guidelines, and checklists, such as recovery procedures
- ❑ Availability of information to organizations through multiple means (web, email, newsletters, manuals, awareness, training classes, etc.)

Scoring Criteria	Yes	No	Evidence
Required			
4.3.1.01 Control: A process is defined for developing and distributing guidelines.	❒	❒	
4.3.1.02 Control: Personnel are trained in the process for developing and distributing guidelines.	❒	❒	
4.3.1.03 Activity: Incident management personnel develop and/or distribute response guidelines to constituents.	❒	❒	
4.3.1.04 Activity: Incident management personnel perform routine and as-needed reviews and updates of response guidelines.	❒	❒	
Recommended Best Practices			
4.3.1.05 Quality: Incident management personnel verify or receive feedback on the constituents' use of guidelines, checklists, and procedures.	❒	❒	
Institutional and Quality Improvement			
4.3.1.06 Control: Documented procedures exist for distributing procedures, guidelines, and checklists to the organization.	❒	❒	
4.3.1.07 Quality: A process and criteria exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	
4.3.1.08 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	Met (all Required indicators have Yes answers)	❒	Not Met (one or more Required indicators have a No answer)	❒
Not Applicable		❒	Not Observed	❒

Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement

- Gather and analyze feedback from the organization on the usefulness of the information.
- Use multiple means of delivering the information, which may be preferable to relying on a single communications mechanism. Choose the mechanism most appropriate for the information being conveyed.

4.3 INCIDENT RESPONSE

4.3.2 Incidents are resolved. **Priority I**

Clarification

This capability focuses on the organization's ability to resolve incidents. Resolution of incidents typically includes containment of the damage caused by an incident, eradication of the cause(s) (to prevent a repeat occurrence), and/or recovery of the affected networks, systems, and information. A goal behind these response actions is to return the affected systems to operation but in a more secure state than before the incident occurred. Recognize that organizational circumstances may limit or constrain what types of resolution can be performed (e.g., some systems may not be allowed to be removed from the network or patched). Capability 4.3.5 addresses verification of incident closure.

The goal of containment is to block the access of the intruder and to limit the damage the intruder can do. Containment strategies will vary for different types of incidents. The actual methods of containment will vary depending on the systems or information affected. Incident management personnel and first responders need to be aware of the impacts, benefits, and drawbacks of different containment actions (for example, the loss of potential evidence that may result from powering off a system, or the possibility that an attack may be programmed to cause additional damage if a compromised system is disconnected from the network).

Eradication of the underlying causes of an incident is important to prevent the attacker from regaining access, as well as to prevent other, unrelated attackers from doing the same. Eradication can include a number of steps, such as installing appropriate patches to prevent the exploitation of vulnerabilities, making configuration changes, changing passwords, providing guidance/education/training to users, and so forth.

Recovery of the affected systems can also include a number of steps in accordance with the damage that has occurred (or the potential damage posed). This can include rebuilding a system from original media (in case of any Trojan horse programs or backdoors installed by the intruder), installing security patches, and restoring other data from backups.

Team Guidance

Depending on the organization, different groups or individuals may have different roles in the process of containing, eradicating, and recovering an incident. Incident management personnel may be actively involved in these activities, or they may merely provide guidance or advice to system owners about performing these actions. The assessment team should ensure that the roles and responsibilities for conducting these response actions are defined.

If incident management personnel do not directly perform any containment, eradication, and recovery activities, they should provide guidance or advice to those who do. Such guidance offered might overlap with other information that the organization provides in capability 4.3.1. Note that this capability may not be applicable to some organizations, such as coordinating CSIRTs.

See the corresponding sections in NIST SP 800-61 Rev 2 (below) for further guidance.

References

Regulatory References:

FISMA Sec 3544 *Federal agency responsibilities* (b)(7) [OLRC 2003]

> "(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] to provide information security for the information and information systems that support the operations and assets of the agency […] that includes— […]
>
> (7) procedures for detecting, reporting, and responding to security incidents, consistent with standards and guidelines issued pursuant to section 3546(b) [National Security Systems] […]"

Guidance References:

NIST SP 800-61 Rev 2 *Computer Security Incident Handling Guide* [Cichonski 2012]

> "Sec. 3.3 Containment, Eradication, and Recovery
> [p 35-37]
>
> 3.3.1 Choosing a Containment Strategy
>
> Containment is important before an incident overwhelms resources or increases damage. Most incidents require containment, so that is an important consideration early in the course of handling each incident.
>
> Containment strategies vary based on the type of incident. […]
>
> Organizations should create separate containment strategies for each major incident type, with criteria documented clearly to facilitate decision-making.
>
> 3.3.4 Eradication and Recovery
>
> […]
>
> Eradication and recovery should be done in a phased approach so that remediation steps are prioritized. For large-scale incidents, recovery may take months; the intent of the early phases should be to increase the overall security with relatively quick (days to weeks) high value changes to prevent future incidents. The later phases should focus on longer-term changes (e.g., infrastructure changes) and ongoing work to keep the enterprise as secure as possible."

NIST SP 800-53 Rev. 4 *Security and Privacy Controls for Federal Information Systems and Organizations* [NIST 2013]

> "IR-4 INCIDENT HANDLING
>
> **Control:** The organization:
>
> a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery […]
>
> Control Enhancements:
>
> (1.) […]
>
> (2.) The organization includes dynamic reconfiguration of [Assignment: *organization-defined information system components*] as part of the incident response capability.
>
> Enhancement Supplemental Guidance: Dynamic reconfiguration includes, for example, changes to router rules, access control lists, intrusion detection/prevention system parameters, and filter rules for firewalls and gateways…

(3.) The organization identifies [Assignment: *organization-defined classes of incidents*] and [Assignment: *organization-defined actions to take in response to classes of incidents*] to ensure continuation of organizational missions and business functions.
(4.) […]
(5.) The organization implements a configurable capability to automatically disable the information system if [Assignment: *organization-defined list of security violations*] are detected."

Organization Response

Examples of Evidence Sought

- ❑ Documented strategies for containing different types of incidents
- ❑ Documented criteria or considerations for determining an appropriate containment strategy
- ❑ A decision matrix or mechanism used for quickly determining a containment strategy
- ❑ "First responder" guidelines for detected/suspected incidents that provide guidance to end users or administrators on what to do (or what not to do)
- ❑ Suggested timeframes for conducting containment, eradication, or recovery actions
- ❑ Checklists or steps for recovering systems
- ❑ Repository of media to be used for restoring OSs and applications on compromised systems
- ❑ Sample incident records that document the containment, eradication, and recovery steps taken

Scoring Criteria	Yes	No	Evidence
Required			
4.3.2.01 Control: Criteria are defined for determining the appropriate response strategy and the circumstances under which they can or cannot be used.	❒	❒	
4.3.2.02 Control: Methods are defined for incident containment, eradication, and recovery based on context.	❒	❒	
4.3.2.03 Control: Personnel are trained appropriately in processes and relevant technologies.	❒	❒	
4.3.2.04 Activity: As a part of resolution, a plan of action is determined.	❒	❒	
4.3.2.05 Activity: Incidents are contained according to organizational guidelines.	❒	❒	

4.3.2.06 Activity: Compromised systems and information are recovered in accordance with organizational guidelines.	❒	❒	
Recommended Best Practices			
4.3.2.07 Activity: The CSIRT verifies that incidents are contained, the underlying causes are identified and mitigated, and that compromised systems and information are recovered in accordance with CSIRT or constituent guidelines.	❒	❒	
4.3.2.08 Quality: Incident containment, eradication, and recovery procedures or guidelines are reviewed and updated as needed (at least annually).	❒	❒	
Institutional and Quality Improvement			
4.3.2.09 Control: Documented incident containment procedures, guidelines, or methods are documented for different types of incidents.	❒	❒	
4.3.2.10 Control: Documented incident eradication procedures or guidelines exist.	❒	❒	
4.3.2.11 Control: Documented system recovery procedures or guidelines exist.	❒	❒	
4.3.2.12 Quality: A process and criteria exist for evaluating the quality of performance and artifacts associated with this activity.	❒	❒	
4.3.2.13 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒	
Not Applicable		❒	**Not Observed**	❒	
Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes
Suggestions for Improvement
None

4.3 INCIDENT RESPONSE

4.3.3 Incident management personnel coordinate incident response across stakeholders.

Priority I

Clarification

This capability focuses on the enterprise-wide and external coordination that an organization performs among the various staff or groups that have roles and responsibilities in incident response activities. These can include internal and external groups such as other CSIRTs or external experts. Coordination with these groups occurs to share information and response actions on intrusions, attacks, and suspicious activities. Depending on the organizational structure or model used for their incident response team, this coordination may be led by a centralized response team or across distributed response teams.

Although the NIST SP 800-61 Rev 2 *Computer Security Incident Handling Guide* identifies incident response "coordination" only with external parties (see Section 4), similar coordination with internal groups is equally important. An organization's incident response team or other incident management personnel should coordinate the response among the appropriate internal individuals or groups that have an incident response role (e.g., management, IT staff, Legal department, HR, Public Affairs, Physical Security), as needed.

Note that this capability is related to other response capabilities for reporting incidents to management (see capability 4.1.2) and providing alerts and warnings (see capability 4.3.4). Capability 4.1.3 is similar in that it focuses on reporting incidents to and coordinating with external organizations.

Team Guidance

The assessment team should look for evidence that the IM function understands the requirements for internal and external coordination and information-sharing, and that the organization conducts these activities in a consistent, accurate, timely, and complete manner.

References

Regulatory References: None

Guidance References: None

[indirect]

NIST SP 800-61 Rev 2 *Computer Security Incident Handling Guide* [Cichonski 2012] [p 17-18]

> "Sec. 2.4.4 Dependencies within Organizations
>
> It is important to identify other groups within the organization that may need to participate in incident handling so that their cooperation can be solicited before it is needed. Every incident response team relies on the expertise, judgment, and abilities of others, including:
>
> - Management. […]
> - Information Assurance. […]
> - IT Support. […]
> - Legal Department. […]

- Public Affairs and Media Relations. […]
- Human Resources. […]
- Business Continuity Planning. […]
- Physical Security and Facilities Management. […]

[p 33-34]

Sec. 3.2.7 Incident Notification

When an incident is analyzed and prioritized, the incident response team needs to notify the appropriate individuals so that all who need to be involved will play their roles. Incident response policies should include provisions concerning incident reporting—at a minimum, what must be reported to whom and at what times (e.g., initial notification, regular status updates). The exact reporting requirements vary among organizations, but parties that are typically notified include:

- CIO
- Head of information security
- Local information security officer
- Other incident response teams within the organization
- External incident response teams (if appropriate)
- System owner
- Human resources (for cases involving employees, such as harassment through email)
- Public affairs (for incidents that may generate publicity)
- Legal department (for incidents with potential legal ramifications)"

NIST 800-53 Rev 4 DRAFT. *Computer Security and Privacy Controls for Federal Information Systems and Organizations* [NIST 2013]

"IR-4 INCIDENT HANDLING

Control: The organization:

(a.) Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;

(b.) Coordinates incident handling activities with contingency planning activities;

Control Enhancements:

(7) INCIDENT HANDLING | INSIDER THREATS - INTRA-ORGANIZATION COORDINATION

The organization coordinates incident handling capability for insider threats across [Assignment: organization-defined components or elements of the organization].

Supplemental Guidance: Incident handling for insider threat incidents (including preparation, detection and analysis, containment, eradication, and recovery) requires close coordination among a variety of organizational components or elements to be effective. These components or elements include, for example, mission/business owners, information system owners, human resources offices, procurement offices, personnel/physical security offices, operations personnel, and risk executive (function). In addition, organizations may require external support from federal, state, and local law enforcement agencies."

Organization Response

Examples of Evidence Sought			
❑ Documented, accurate POC lists for other internal incident management personnel or groups ❑ Records of coordination or information-sharing among internal groups ❑ Observations or demonstrations of communication channels or mechanisms for coordination and information-sharing ❑ Secure communications mechanisms to share information with appropriate internal groups in a manner that is commensurate with the sensitivity of the information (e.g., encrypted email, PGP/GnuPG, S/MIME, PKI, STE, secure FAX, secure portal, SIPRNET)			
Scoring Criteria	Yes	No	Evidence
Required			
4.3.3.01 Control: A department, group, or manager in the organization is designated as having responsibility for coordinating response activities across the enterprise and with external groups.	❒	❒	
4.3.3.02 Control: Criteria exist for when and how to share information with other groups.	❒	❒	
4.3.3.03 Control: A defined process exists for coordinating response activities and sharing information with appropriate groups.	❒	❒	
4.3.3.04 Control: Personnel are appropriately trained in the processes and relevant technologies for coordinating response activities and sharing information with other groups.	❒	❒	
4.3.3.05 Activity: Incident management personnel coordinate incident response activities among other groups.	❒	❒	
Recommended Best Practices			
4.3.3.06 Activity: Personnel participate in meetings, conference calls, technical exchanges, and so forth to improve communication channels with internal and external organizations (IT staff, HR, Legal department, Public Affairs, other CSIRTs, etc.).	❒	❒	
Institutional and Quality Improvement			
4.3.3.07 Control: Documented procedures exist for coordinating response activities and sharing information about different types of incidents, including assigned roles, responsibilities, updated POCs, and information-sharing channels or mechanisms.	❒	❒	

4.3.3.08 Control: Personnel are aware of, knowledgeable of, and consistently follow the procedures for this activity.	❒	❒	
4.3.3.09 Quality: A process and criteria exist for evaluating the quality of performance and artifacts associated with this activity.	❒	❒	
4.3.3.10 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒	
Not Applicable		❒	**Not Observed**	❒	

Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement
None

4.3 INCIDENT RESPONSE

4.3.4 Incident management personnel create alerts and warnings, and distribute them as needed.

Priority I

Clarification

This capability addresses the ability of the IM function to provide complete, abbreviated, or abstracted event or incident reports, with threat and vulnerability notifications, alerts, or warnings to constituents or other external parties as required.

Part of an effective incident management process is the ability to quickly disseminate the right information to the right people at the right time. The constituency and individuals need to understand what threats or vulnerabilities might impact them, the associated level of risk, and how to protect against or mitigate them.

Incident management personnel work to provide such notifications and warnings to promote awareness of threats and malicious activity and to help support organizational response actions. Depending on the mission of the incident management function, alerts and warnings may be shared with other relevant stakeholders and external parties.

Notifications, reports, and warnings should be distributed in a manner commensurate with the classification of the information related to the activity. Sensitive and classified activity should only be handled via appropriate secure mechanisms and within the appropriate facilities.

Note that another capability (4.1.2) focuses on reporting incidents and events to management within the organization. This capability overlaps capability 4.1.2 and expands the provision of other notifications (not only incident reports) to other organizational groups beyond management alone.

Team Guidance

The team should look for evidence of notifications and warnings going to organizational stakeholders or other relevant external parties. The teams should also look to see that the information passed is handled according to its classification. The methods for distributing alerts and warnings include emails, websites, telephone calls, in-person conversations, voicemail messages, paper notices, SMS, blogs, and other social media. The communication plan (refer to capability 1.2.1) should define the criteria for communicating with the organization and external parties, as well as define any requirements, policies, and guidance for performing this communication.

References

Regulatory References: None

Guidance References:

NIST SP 800-61 Rev 2 *Computer Security Incident Handling Guide* [Cichonski 2012]

> [p 18]
> "Sec. 2.5 Incident Response Team Services
> Advisory Distribution. A team may issue advisories within the organization regarding new vulnerabilities and threats. Automated methods should be used whenever appropriate to

disseminate information; for example, the National Vulnerability Database (NVD) provides information via XML and RSS feeds when new vulnerabilities are added to it. Advisories are often most necessary when new threats are emerging, such as a high-profile social or political event (e.g., celebrity wedding) that attackers are likely to leverage in their social engineering. Only one group within the organization should distribute computer security advisories to avoid duplicated effort and conflicting information.

[p 33-34]
Sec 3.2.7 Incident Notification
When an incident is analyzed and prioritized, the incident response team needs to notify the appropriate individuals so that all who need to be involved will play their roles.

During incident handling, the team may need to provide status updates to certain parties, even in some cases the entire organization. The team should plan and prepare several communication methods, including out-of-band methods (e.g., in person, paper), and select the methods that are appropriate for a particular incident."

Organization Response

Examples of Evidence Sought

- ❑ Copies of threats, warnings, advisories, event/incident notifications, etc. that were sent to organizational stakeholders, constituents, or other external parties
- ❑ Mechanisms, with instructions and examples, for notifying the organization about current or potential events/incidents (e.g., email, web, mailing list, text, SMS)
- ❑ Secure communication mechanisms commensurate with the sensitivity of the information (e.g., PGP, GnuPG, S/MIME, PKI, STE, secure FAX, secure portal)
- ❑ Documented and up-to-date organizational POC lists with appropriate contact information and alternates
- ❑ Documented sources for information-gathering on current and potential threats and attacks

Scoring Criteria	Yes	No	Evidence
Required			
4.3.4.01 Control: Criteria exist for disseminating information, including defining who receives what data and when.	❒	❒	
4.3.4.02 Control: Documented policies or guidance exist that define the requirements for notifying constituents (e.g., types, security levels, communications mechanisms).	❒	❒	
4.3.4.03 Control: Personnel are appropriately trained in the relevant processes and technologies.	❒	❒	

4.3.4.04 Activity: Notifications and reports related to current or potential threats, vulnerabilities, and incidents are sent to the appropriate POCs within the constituency and to relevant external parties as outlined by SLAs or organizational requirements.	❒	❒	
4.3.4.05 Activity: Sensitive and classified information is handled and stored according to legal and organizational requirements.	❒	❒	
Recommended Best Practices			
4.3.4.06 Prerequisites: Documented requirements exist for levels of communication security.	❒	❒	
4.3.4.07 Control: Predefined countermeasures or protection strategies are documented and distributed.	❒	❒	
4.3.4.08 Control: Guidance exists for assessing the level of risk and corresponding impact relative to the constituency.	❒	❒	
4.3.4.09 Activity: Reporting and notification guidelines are reviewed at least annually within the organization and updated as needed.	❒	❒	
Institutional and Quality Improvement			
4.3.4.10 Control: Documented procedures and mechanisms exist for notifying the constituency and relevant external parties (e.g., required content, timeframes, security levels, secure communication).	❒	❒	
4.3.4.11 Quality: Personnel are aware of, knowledgeable of, and consistently follow the procedures.	❒	❒	
4.3.4.12 Quality: A process and criteria exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	
4.3.4.13 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒

Not Applicable	❒	Not Observed	❒

Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement
None

4.3 INCIDENT RESPONSE

4.3.5 Incident management personnel verify that a response is implemented, as appropriate, and that the incident is closed, in accordance with organizational guidance.

Priority I

Clarification

This capability focuses on incident management personnel ensuring that any information or relevant metrics that must be gathered have been documented (e.g., all appropriate fields in the incident tracking system/database have been filled out), that all appropriate response actions have been completed, and that criteria for incident closure have been met, before the incident is marked as closed. The incident management function verifies that any recommended response activities have been implemented. This can include actions for containment, eradication, and recovery of the affected systems and information. Verification can be obtained through a variety of procedures or mechanisms, such as a simple follow-up email from the owners or administrators of the affected systems that confirms appropriate response actions have been taken; formal checking (e.g., via vulnerability scanning or penetration testing) that the conditions that enabled an incident to occur have been mitigated; or additional monitoring to look for future related activity. The incident response actions taken should be documented in the incident response records.

Team Guidance

Verification of the implemented response may not be part of the incident management function, for example this may be an audit function. If this capability is performed by a different group, the assessment team should assess that group.

References

Regulatory References: None

Guidance References: None

[indirect]

NIST SP 800-61 Rev 2 *Computer Security Incident Handling Guide* [Cichonski 2012]

> [p 42]
> "Table 3-5. Incident Handling Checklist
> […]
> 7. Recover from the incident
> 7.1 Return affected systems to an operationally ready state
> 7.2 Confirm that the affected systems are functioning normally
> 7.3 If necessary, implement additional monitoring to look for future related activity"

Organization Response

Examples of Evidence Sought			
❑ Follow-up emails or other communication records that verify that response actions (including containment, eradication, and recovery, as needed) have been completed ❑ Records that verify the causes of an incident have been corrected or mitigated ❑ Documented results of post-incident vulnerability scans or penetration tests ❑ Records that show increased monitoring of affected systems following an incident ❑ Documented policies or procedures that address response verification and/or incident closure steps ❑ Observation of personnel performing verification activities ❑ Observation of personnel closing an incident			
Scoring Criteria	Yes	No	Evidence
Required			
4.3.5.01 Control: Defined criteria exist for what constitutes incident closure.	❒	❒	
4.3.5.02 Control: A documented process exists for verifying incident response actions.	❒	❒	
4.3.5.03 Control: A documented process exists for closing incidents.	❒	❒	
4.3.5.04 Activity: Personnel verify that the recommended response is implemented.	❒	❒	
4.3.5.05 Activity: Implementation actions taken regarding incident response are recorded in the incident tracking system.	❒	❒	
4.3.5.06 Activity: Incident reports are closed in accordance with organizational guidance and criteria.	❒	❒	
Recommended Best Practices			
4.3.4.07 Control: A documented policy exists that authorizes incident management personnel to test or verify (e.g., through vulnerability scanning or penetration testing) that vulnerabilities or weaknesses have been corrected following an incident.	❒	❒	
4.3.5.08 Activity: Incidents records are reviewed before closure for accuracy and completeness of information, and that all needed actions have been taken.	❒	❒	

4.3.4.09 Activity: Incident management personnel independently check or confirm that vulnerabilities or causes of an incident have been corrected prior to closure.	❒	❒	
Institutional and Quality Improvement			
4.3.5.10 Control: Documented procedures exist for conducting this activity.	❒	❒	
4.3.5.11 Quality: Personnel are aware of, knowledgeable of, and consistently perform the procedures.	❒	❒	
4.3.5.12 Quality: A process and criteria exist for evaluating how this activity is performed and the quality of its artifacts.	❒	❒	
4.3.5.13 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒
Not Applicable		❒	**Not Observed**	❒

Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement
None

4.3 INCIDENT RESPONSE

4.3.6 Postmortem reviews of significant incidents are conducted, and lessons learned are identified and acted upon, as appropriate.

Priority I

Clarification

This capability ensures that postmortem meetings or reviews are held after significant incidents. The organization will need to define what "significant" means to them. The intent of these reviews is to identify any issues encountered or lessons learned, to propose areas for improvement, and to act on these findings or recommendations.

NIST SP 800-61 Rev 2, *Computer Security Incident Handling Guide*, Sections 3.4.1 and 3.4.2 provide detailed guidance and suggestions for this activity. For example, "Lessons learned meetings provide other benefits. Reports from these meetings are good material for training new team members by showing them how more experienced team members respond to incidents. Updating incident response policies and procedures is another important part of the lessons learned process. Post-mortem analysis of the way an incident was handled will often reveal a missing step or an inaccuracy in a procedure, providing impetus for change. Because of the changing nature of information technology and changes in personnel, the incident response team should review all related documentation and procedures for handling incidents at designated intervals. [NIST 2012]."

Team Guidance

The assessment team should look for any documentation or records that demonstrate the IM function identifies lessons learned following major incidents and the recommendations from such reviews are implemented.

Refer to NIST SP 800-61 Rev 2, Sections 3.4.1 and 3.4.2 (see below) for detailed guidance regarding post-incident lessons learned and questions to be answered during this activity. (Also note the guide states that while the learning and improving part of incident response is one of the most important parts, it is "also the most often omitted.")

Note that Protect capability 2.3.1 addresses lessons learned from operational exercises, whereas this capability focuses on similarly conducting lessons learned after significant incidents.

References

Regulatory References: None

Guidance References:

NIST SP 800-61 Rev 2 *Computer Security Incident Handling Guide* [Cichonski 2012]

> [p. 38-39]
> "Sec. 3.4.1 Lessons Learned
> One of the most important parts of incident response is also the most often omitted: learning and improving. Each incident response team should evolve to reflect new threats, improved technology, and lessons learned. Holding a "lessons learned" meeting with all involved parties after a major incident, and optionally periodically after lesser incidents as resources permit, can be extremely helpful in improving security measures and the incident handling

process itself. Multiple incidents can be covered in a single lessons learned meeting. This meeting provides a chance to achieve closure with respect to an incident by reviewing what occurred, what was done to intervene, and how well intervention worked. The meeting should be held within several days of the end of the incident. Questions to be answered in the meeting include

- Exactly what happened, and at what times?
- How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

[p 39-41]
Sec. 3.4.2 Using Collected Incident Data
Lessons learned activities should produce a set of objective and subjective data regarding each incident."

Organization Response

Examples of Evidence Sought

- ❑ Records of post-incident meetings or reviews after significant incidents that identify lessons learned, issues encountered, or areas for improvement
- ❑ Documentation showing implemented changes or incorporated lessons learned following a postmortem incident review
- ❑ Post-incident follow-up reports that provide information or metrics for making incident response process improvements

Scoring Criteria	Yes	No	Evidence
Required			
4.3.6.01 Control: Criteria exist for identifying significant incidents that require postmortems.	❒	❒	

4.3.6.02 Activity: Lessons learned meetings/reviews are held after significant incidents.	❒	❒	
4.3.6.03 Activity: Results of the postmortem reviews identify incident response actions that worked well and those that could have been improved.	❒	❒	
4.3.6.04 Activity: Findings or recommendations from incident response postmortem reviews are implemented.	❒	❒	
Recommended Best Practices			
4.3.6.05 Control: A list of questions to be answered during postmortem incident reviews exists.	❒	❒	
4.3.6.06 Activity: Any new vulnerabilities or other weaknesses identified from the incident are recorded in the organization's vulnerability or other appropriate tracking system.	❒	❒	
4.3.6.07 Activity: Any vulnerabilities identified from the incident are addressed through normal patch or configuration management processes.	❒	❒	
4.3.6.08 Activity: Any changes to the constituent infrastructure based on incident response lessons learned are submitted through the appropriate change management process.	❒	❒	
Institutional and Quality Improvement			
4.3.6.09 Control: Documented procedures exist for conducting this activity.	❒	❒	
4.3.6.10 Quality: Personnel are aware of, knowledgeable of, and consistently perform the procedures.	❒	❒	
4.3.6.11 Quality: A process and criteria exist for evaluating the how this activity is performed and the quality of its artifacts.	❒	❒	
4.3.6.12 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒
Not Applicable		❒	**Not Observed**	❒

Evidence Collected					
Document Review		Interviews		Direct Observation	
Notes					
Suggestions for Improvement					
None					

SUSTAIN: SECTION 5 OF INCIDENT MANAGEMENT CAPABILITIES

Sustain focuses on the ability of the organization to identify and implement what needs to be in place to continue to provide a timely, effective, and sustained incident management function. During Prepare, the incident management function is established with the mission, objectives, plans, policies, procedures, and basic tools. During Sustain, the focus shifts to maintaining skilled staff, technological resources, and other processes and equipment needed to improve the IM function.

Also required are the supporting infrastructure, controls, supporting mechanisms, artifacts, and quality measures that enable incident management personnel to perform their functions. In this regard, the appropriate contracts, MOUs, and SLAs should be should be established that define roles and responsibilities; financial planning and budgeting processes to sustain operations over time; training and educational opportunities for staff; program management plans; and other important items.

Part of any sustainment capability includes improving the overall effectiveness of the operations. This is also true in the case of a CSIRT or incident management function. As appropriate responses are made, lessons learned should be captured and fed into process improvements.

The Sustain category includes these subcategories and capabilities:

- **5.1. MOUs and Contracts—**MOUs, MOAs, LOAs (Letters of Agreement), SLAs, or contracts that formalize activities and define services are provided by the incident management function to establish correct expectations for operations.
  - 5.1.1. A list of incident management services provided by the designated incident management function is documented.
  - 5.1.2. The constituency provides advance notification of all changes or planned outages to their networks.
  - 5.1.3. Formal agreements exist for managing IM activities with third parties across the supply chain.
- **5.2. Project/Program Management**—This management provides guidance and oversight for continued incident management operations, financial planning, business resumption, and other relevant activities.
  - 5.2.1. A financial plan exists for incident management activities.
  - 5.2.2. A workforce plan exists for incident management personnel.
  - 5.2.3. A personnel security plan exists for incident management personnel.
  - 5.2.4. A quality assurance (QA) program exists to ensure the quality of provided products and services.
  - 5.2.5. An established plan exists to ensure continuity of operations for incident management.
  - 5.2.6. The effectiveness of the incident management function in meeting its mission is routinely evaluated and improved.
- **5.3. IM Technology Development, Evaluation, and Implementation**—These capabilities evaluate the ability of the organization to test software and analyze impacts prior to

implementing them in production networks, and examine new technologies that are incorporated into the infrastructure.

5.3.1. The incident management function has the tools it needs to meet its mission.

5.3.2. Software tools are tested for use within the incident management environment.

5.3.3. The IT infrastructure for incident management is adequate to support incident management operations.

5.4. Personnel—To meet the changing needs of the organization, this capability focuses on ensuring there is a cadre of personnel with the required knowledge, skills, and abilities to perform the work and to continue to develop professionally.

5.4.1. A training program exists for incident management personnel.

5.4.2. Support for professional development exists for incident management personnel.

5.5. Security Administration—This capability covers physical security measures and operations security (OPSEC).

5.5.1. Physical protective measures are in place to protect incident management IT systems, facilities, and personnel.

5.5.2. An operations security (OPSEC) program exists.

5.6. IM Information Systems—This capability ensures the organization utilizes a defense-in-depth approach for hardening systems and networks (e.g., data protection, monitoring, risk assessments, vulnerability scanning, patch management strategies, communications methods) used for incident management capabilities.

5.6.1. An inventory exists of mission-critical incident management systems, data, and information.

5.6.2. Defense-in-depth strategies and methodologies exist for hardening the incident management computer networks and systems.

5.6.3. Processes and technologies exist to support the confidentiality, integrity, and availability of incident management data and information.

5.6.4. Network security monitoring is performed on all incident-management-related networks and systems.

5.6.5. Security risk assessments (RAs) are performed on the incident management function.

5.6.6. Vulnerability assessments are performed on incident management systems and networks.

5.6.7. A patch management program is in place for the incident management systems.

5.6.8. More than one communications system or mechanism (other than email) exists for receiving and distributing notifications, information about new viruses, incidents, vulnerabilities, threats, and other kinds of warnings.

5.1 MOUS AND CONTRACTS

5.1.1 A list of incident management services provided by the designated incident management function is documented.

Priority II

Clarification

The intent of this capability is to ensure that the organization clearly sets the expectations regarding what incident management services will be provided, to whom, and by whom, any associated costs, and any other related information. Setting these expectations early helps avoid confusion and misunderstandings later. Once the list of services is identified, documenting it ensures that the designated incident management function or CSIRT and the constituents know how to interact with each other.

This list should detail the services provided and the associated available resources for both normal and emergency situations.

Any list of services should also include a description of the level of service provided. For example, if an incident response service is provided, will the team come on-site and perform the mitigation, or will they only suggest potential mitigations by phone?

Team Guidance

The documented list can be either formal (such as a written SLA) or informal (such as an email message). The documentation does not have to be a list. It could be a more general description of services documented in a CONOPS or an incident management plan.

References

Regulatory References: None

Guidance References: None

[indirect]

NIST SP 800-61 Rev 2 *Computer Security Incident Handling Guide* [Cichonski 2012]

> "Sec 2.5 Incident Response Team Services
> [p 2-14]
>
> […] it is fairly rare for a team to perform incident response only.
>
> Sec 2.6 Recommendations
> Determine which services the team should offer."

Organization Response

Examples of Evidence Sought			
❑ Copy of written agreement (e.g., MOU, SLA, MOA, LOA) that has been signed by management, or an official webpage or other document that clearly states the designated services ❑ Documented list of services ❑ Observation of mechanism for informing the organization of the services provided (e.g., website, mailing list showing the list of services, CONOPS, or incident management plan)			
Scoring Criteria	Yes	No	Evidence
Required			
5.1.1.01 Control: A defined process exists for determining and maintaining the list of services.	❒	❒	
5.1.1.02 Activity: The incident management services to be provided are determined.	❒	❒	
5.1.1.03 Activity: A list of defined incident management services provided to the organization is documented and maintained.	❒	❒	
Recommended Best Practices			
5.1.1.04 Control: If another service provider, contractor, or external group provides incident management services, those arrangements are documented in the agreement with the organization.	❒	❒	
5.1.1.05 Activity: The list of services should be available to the organization in multiple ways such as via email, a public website of reporting guidelines, an SLA, an MOU or a brochure.	❒	❒	
5.1.1.06 Activity: Personnel work with the organization to set and manage its expectations of what services can and will be delivered.	❒	❒	
Institutional and Quality Improvement			
5.1.1.07 Quality: A process and criteria exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	
5.1.1.08 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒	
Not Applicable		❒	**Not Observed**	❒	
Evidence Collected					
Document Review		Interviews		Direct Observation	
Notes					
Suggestions for Improvement					
• Build mechanisms for educating constituents about the incident management services. This task might include building such information into introductory materials, incident reporting guidance, employee handbooks, and other similar materials.					

5.1 MOUS AND CONTRACTS

5.1.2 The constituency provides advance notification of all changes or planned outages to their networks.

Priority III

Clarification

The intent of this capability is to ensure that incident management personnel are updated on all constituents' infrastructure changes, such as configuration changes, scheduled power outages, and maintenance on critical network assets. An agreement should stipulate exactly what changes require notification. Without this information, incident management personnel may not be able to adequately assess the validity of a given event or incident report. Such notifications help incident management personnel determine when reported behavior may have been caused by normal maintenance or configuration updates, rather than by malicious intruder activity that disables part of the constituent network. These notifications also facilitate an accurate inventory of system and network components.

The agreement, either written or informal, should exist to ensure that the incident management function and constituents know how to keep each other informed. This capability is focused on ensuring that the constituents manages the configuration of its network assets; understands the current status of critical systems and data; maintains schedules and plans of network outages and changes; and notifies the incident management personnel about any changes or planned outages to its systems and networks. Configuration management change boards are also a source of scheduled or planned change information.

Team Guidance

When assessing this capability, the team should determine whether constituents notify incident management personnel about infrastructure changes.

If the constituents are not responsible for making changes to their networks, this capability should be assessed against the group that does perform that function.

References

Regulatory References: None

Guidance References: None

Organization Response

Examples of Evidence Sought

- ❑ Formal or informal agreement document
- ❑ Examples of alerts or notifications of outages
- ❑ Observation or demonstration of a change management system or other mechanism used to provide alerts of outages

Scoring Criteria	Yes	No	Evidence
Required			
5.1.2.01 Control: An informal or formal agreement stipulates what types of changes will be reported, along with the POCs to be notified and notification timelines.	❒	❒	
5.1.2.02 Activity: Constituents give advance warning about all network changes, maintenance, and outages.	❒	❒	
Recommended Best Practices			
5.1.2.03 Control: Incident management support during maintenance or extended outages is defined.	❒	❒	
Institutional and Quality Improvement			
5.1.2.04 Quality: Incident management personnel are aware of and knowledgeable about the contents of the agreement.	❒	❒	
5.1.2.05 Quality: Organizational personnel are aware of and knowledgeable about the contents of the agreement.	❒	❒	
5.1.2.06 Quality: Notification occurs in compliance with agreement terms, such as within the proper timeframe.	❒	❒	
5.1.2.07 Quality: A process and criteria exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	
5.1.2.08 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒
Not Applicable		❒	**Not Observed**	❒

Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement
• Incorporate incident management personnel into any constituent change management system and announcements. This works best when incident management personnel can provide input and recommend changes. • Implement an automated change management system or inventory to provide an efficient tool for archiving such infrastructure changes and allowing them to be searched and reviewed easily.

5.1 MOUS AND CONTRACTS

5.1.3 Formal agreements exist for managing IM activities with third parties across the supply chain.

Priority I

Clarification

The intent of this capability is to ensure that the incident management function works effectively with contractor organizations throughout the organization's supply chain. This can include MSSPs, cloud service providers, off-site storage providers, data centers, and so forth. This capability addresses how the incident management function performs the following activities with third parties:

- contracts for services
- communicates status information and reporting information
- coordinates service delivery
- protects its system and networks from threats introduced by third parties
- deals with incidents across the supply chain
- establishes requirements for bi-directional event and incident reporting and handling

This capability assumes that the incident management function has made a well-informed business decision to engage with third parties and understands the risks of doing so.

Team Guidance

When assessing this capability, the team should review contracts and agreements with third parties across the organization's supply chain. The team should determine whether contracts and agreements define roles and responsibilities related to service delivery between the incident management function and third parties. The team should look for plans that are in place for communicating and coordinating activities with third parties, protecting third-party data, managing incidents that affect contractors, and protecting the organization's data from third parties.

The team should also look for processes used to develop, review, update, and terminate agreements with third parties (e.g., SLAs, MOUs, MOAs, and LOAs).

References

Regulatory References: None

[indirect]

FIPS 200 *Minimum Security Requirements for Federal Information and Information Systems* [NIST 2006]

> "Organizations must (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization."

Guidance References:

NIST 800-53 Rev. 4 *Security and Privacy Controls for Federal Information Systems and Organizations* [NIST 2013]

"SA-12 SUPPLY CHAIN PROTECTION

Control: The organization protects against supply chain threats to the information system, system component, or information system service by employing [*Assignment: organization-defined security safeguards*] as part of a comprehensive, defense-in-breadth information security strategy.

Control Enhancements:

1. SUPPLY CHAIN PROTECTION | ACQUISITION STRATEGIES / TOOLS / METHODS: The organization employs [Assignment: organization-defined tailored acquisition strategies, contract tools, and procurement methods] for the purchase of the information system, system component, or information system service from suppliers.

Supplemental Guidance: The use of acquisition and procurement processes by organizations early in the system development life cycle provides an important vehicle to protect the supply chain. Organizations use available all-source intelligence analysis to inform the tailoring of acquisition strategies, tools, and methods. There are a number of different tools and techniques available (e.g., obscuring the end use of an information system or system component, using blind or filtered buys). Organizations also consider creating incentives for suppliers who: (i) implement required security safeguards; (ii) promote transparency into their organizational processes and security practices; (iii) provide additional vetting of the processes and security practices of subordinate suppliers, critical information system components, and services; (iv) restrict purchases from specific suppliers or countries; and (v) provide contract language regarding the prohibition of tainted or counterfeit components. In addition, organizations consider minimizing the time between purchase decisions and required delivery to limit opportunities for adversaries to corrupt information system components or products. Finally, organizations can use trusted/controlled distribution, delivery, and warehousing options to reduce supply chain risk (e.g., requiring tamper-evident packaging of information system components during shipping and warehousing)."

NIST SP 800-144 (Dec. 2011) *Guidelines on Security and Privacy in Public Cloud Computing*

NIST SP 800-145 (Sept. 2011) *The NIST Definition of Cloud Computing*

NIST SP 800-146 (May 2012) *Cloud Computing Synopsis and Recommendations*

Organization Response

Examples of Evidence Sought

- ❑ Copy of written agreements with third parties (e.g., SLAs, MOUs, MOAs, LOAs) that have been signed by management
- ❑ Organizational policies or other documents describing how to engage and work with third parties
- ❑ Observation or demonstration of mechanisms for communicating and coordinating activities with third parties
- ❑ Reports of incidents with third parties that show how the incident was handled or communicated

Scoring Criteria	Yes	No	Evidence
Required			
5.1.3.01 Control: Incident management requirements are defined for any third-party service.	❒	❒	
5.1.3.02 Control: Plans and processes are in place for coordinating activities between the incident management function and any third-party.	❒	❒	
5.1.3.03 Control: Defined processes and guidelines are in place for reporting threats, incidents, and events occurring at third-party to the contract owner.	❒	❒	
5.1.3.04 Activity: Each contractor organization is provided with a detailed agreement (e.g., SLA, MOU).	❒	❒	
5.1.3.05 Activity: Services are delivered and received in accordance with agreements.	❒	❒	
Recommended Best Practices			
5.1.3.06 Control: The incident management function has controls in place for mitigating the risk of security incidents to the organization's systems and networks across the organization's supply chain.	❒	❒	
5.1.3.07 Activity: Requirements and agreements for joint security policies and controls are defined and documented.	❒	❒	
5.1.3.08 Control: The incident management function has defined processes for developing, reviewing, updating, and terminating its agreements.	❒	❒	
5.1.3.09 Control: An exception request process (specified in the agreement) for individual contractors is provided.	❒	❒	
5.1.3.10 Activity: The incident management function has assessed the risks of engaging with third parties.	❒	❒	

Institutional and Quality Improvement			
5.1.3.11 Quality: Incident management personnel are aware of and knowledgeable about the contexts of agreements with contractor organizations throughout the supply chain.	❒	❒	
5.1.3.12 Quality: A process and criteria exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	
5.1.3.13 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒
Not Applicable		❒	**Not Observed**	❒

Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement
None

5.2 PROJECT/PROGRAM MANAGEMENT

5.2.1 A financial plan exists for incident management activities. Priority III

Clarification

The intent of this capability is to address program management efforts related to planning and budgeting for current and future incident management requirements. The incident management arena is highly dynamic and, to be as prepared as possible, the appropriate staff, equipment, and infrastructure must exist. Preparation activities for incident management include training for staff on attack types; incident handling and security tools; and methods and technologies for responding to events and incidents. A sound financial plan helps to ensure that incidents can be managed successfully, both in the near term and future. Without such a plan, an organization cannot ensure continued growth or even continued daily operations for incident management. The financial plan for incident management can be a stand-alone plan, or it can be part of a broader financial plan for the organization. The financial plan should be in compliance with all applicable regulatory requirements.

Team Guidance

This capability refers to the incident management financial plan or to the incident management portion of an organization's broader financial plan. The team should note when some services or functions are provided by contractors or managed service providers. Additional financial plans might exist for each third party (e.g., contractor, managed service provider). The team should also note when the financial plan for incident management is part of a larger financial plan; in that case, it is important to make sure that incident management personnel have some control over what is proposed and incorporated into the larger financial plan.

This function might be outsourced or handled by another part of the organization. In that case, this capability should be applied to that group and its activities.

References

Regulatory References:

FISMA Sec 3544 *Federal agency responsibilities* (c)(2)(A) and (d)(1)(B) [OLRC 2003]

> "(c) AGENCY REPORTING—Each agency shall—
>
> (2) address the adequacy and effectiveness of information security policies, procedures, and practices in plans and reports relating to—
>
> (A) annual agency budgets
>
> (d) PERFORMANCE PLAN—
>
> (1) In addition to the requirements of subsection (c), each agency, in consultation with the Director, shall include as part of the performance plan required under section 1115 of title 31 a description of— […]
>
> (B) the resources, including budget, staffing, and training, that are necessary to implement the program required under subsection (b)."

[indirect]
FISMA Sec 3544 *Federal agency responsibilities* (a)(1)(C)

> "(a) IN GENERAL—The head of each agency shall— […]
>
> (1) be responsible for—
>
> (2) (C) ensuring that information security management processes are integrated with agency strategic and operational planning processes"

Guidance References:

NIST SP 800-61 Rev 2 *Computer Security Incident Handling Guide* [Cichonski 2012]

> "Cost. Cost is a major factor, especially if employees are required to be onsite 24/7. Organizations may fail to include incident response-specific costs in budgets, such as sufficient funding for training and maintaining skills. Because the incident response team works with so many facets of IT, its members need much broader knowledge than most IT staff members. They must also understand how to use the tools of incident response, such as digital forensics software. Other costs that may be overlooked are physical security for the team's work areas and communications mechanisms.
>
> Budget enough funding to maintain, enhance, and expand proficiency in technical areas and security disciplines, as well as less technical topics such as the legal aspects of incident response."

A Step-By-Step Approach on how to Set Up a CSIRT [ENISA, 2006]

> "Developing the Business Plan
> Defining the financial model
> After the analysis a couple of core-services were picked to start with. The next step is to think about the financial model: what parameters of service provision are both suitable and payable."

Organization Response

Examples of Evidence Sought

- ❑ Financial plan documentation, including
  - staffing
  - equipment
  - supporting costs
- ❑ Financial plans for contractors or other outsourced labor, when applicable

Scoring Criteria	Yes	No	Evidence
Required			
5.2.1.01 Activity: Incident management personnel or managers determine, recommend, and control (to the extent possible) current and future budgetary requirements.	❒	❒	
5.2.1.02 Control: A process is defined for developing and maintaining the financial plan.	❒	❒	

5.2.1.03 Activity: An *n*-year financial plan is built.	❒	❒	
Recommended Best Practices			
5.2.1.04 Control: Personnel are trained in financial planning, budgeting techniques and methodologies, and the financial-plan-compliance regulations applicable to their organization.	❒	❒	
5.2.1.05 Activity: The financial plan is reviewed and updated at least annually (to accommodate changing needs in equipment, personnel, policy, procedures, etc.).	❒	❒	
5.2.1.06 Activity: Plan estimates budgetary projections for multiple (ideally three to five) years.	❒	❒	
Institutional and Quality Improvement			
5.2.1.07 Quality: The financial plan is in compliance with organizational regulatory requirements.	❒	❒	
5.2.1.08 Quality: A process and criteria exist for evaluating the quality of the financial plan.	❒	❒	
5.2.1.09 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒	
Not Applicable		❒	**Not Observed**	❒	

Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement
• Ensure that financial plans and budgets include funds for sustaining the overall quality of the incident management function. • Enable staff to keep pace with the changes in technology and usage. Set aside funding for continuing education or refresher courses so incident management personnel can continue to be effective incident handlers. • Ensure that budgets and financial plans include funding for professional development opportunities for incident management personnel. This funding can be used to enhance team members' knowledge and abilities; keep them engaged and energized about incident management work; expand the overall skills and knowledge of the team; and meet requirements for any certifications that might be required for certain incident management personnel or services.

5.2 PROJECT/PROGRAM MANAGEMENT

5.2.2 A workforce plan exists for incident management personnel. Priority II

Clarification

The intent of this capability is to ensure that staffing resources are sufficient to execute the incident management mission. This capability focuses principally on planning staffing needs. Many incident management teams possess a core group of individuals who provide the basic level of incident handling services. Each staff member is expected to have some minimum set of basic skills to do the work and be effective in his or her work responsibilities. The workforce plan needs to take into account how many of each type of staff is needed to provide the list of incident management services and the required clearance. The workforce plan needs to be updated whenever the mission or services to be provided changes.

For example, while all team members are expected to recognize any malware found as part of an incident, only a subset of that staff may have the skills needed to analyze intruder-developed exploit tools; identify and document the impact of resulting attacks; and provide insight to other team members. Thus, it is also important for the team to include or have access to experts with in-depth understanding of the technologies that the team and organization use. These experts, who might be in another part of the organization, can provide technical guidance or advice; they might also provide training and mentoring to other team members. This additional level of expertise is a resource that can help broaden and deepen the team's technical knowledge and capabilities.

When more complex incidents are reported, teams will need to supplement or expand their basic skills to include more in-depth knowledge so they can understand, analyze, and identify effective responses to reported incidents.

The workforce plan should identify current staffing needs and required reachback or surge personnel. *Reachback* means that these personnel will only be activated when needed. Reachback personnel normally exist in other parts of the organization but have the right skills, abilities, and training to be pulled in on an as-needed basis. If incident management services are provided by contractors, reachback or surge support may need to be outlined in a contract or SLA.

Team Guidance

The team should look for an up-to-date workforce plan (which could be part of a larger program management plan) that documents the types and number of personnel required. The plan should document the personnel who are internal and external to incident management; look for evidence of this support in an SLA.

The team should determine who is needed to achieve the incident management mission. The plan should also include a method for reachback or surge support. If reachback is provided by contractors, the team should look for evidence or indications that the organization uses some form of quantitative statistics that can be analyzed and used to extrapolate future staffing needs, such as metrics for when it is time to replace reachback personnel with full-time staff.

References

Regulatory References:

FISMA Sec 3544 *Federal agency responsibilities* (d)(1)(B) [OLRC 2003]

> "(d) PERFORMANCE PLAN—
>
> (1) In addition to the requirements of subsection (c), each agency, in consultation with the Director, shall include as part of the performance plan required under section 1115 of title 31 a description of— […]
>
> (2) (B) the resources, including budget, staffing, and training, that are necessary to implement the program required under subsection (b)."

[indirect]
FISMA 3544 *Federal agency responsibilities* (a)(1)(C)

> "(a.) IN GENERAL—The head of each agency shall— […]
>
> (b.) (1) be responsible for –
>
> (c.) (C) ensuring that information security management processes are integrated with agency strategic and operational planning processes"

Guidance References: None

[indirect]

NIST SP 800-61 Rev 2 *Computer Security Incident Handling Guide* [Cichonski 2012]

> "Sec 2.4.3 Incident Response Personnel
> Members of the incident response team should have excellent technical skills, such as system administration, network administration, programming, technical support, or intrusion detection."

Good Practice Guide for Incident Management [ENISA, 2010]

> "6—Roles
> For incident management to be successful, it is essential to carefully consider the roles within a CERT and to tailor these to your specific mission, constituency and environment. A CERT can be a virtual team with no formal members and with tasks distributed between different employees in various company departments such as the network operations center, internal IT security team, legal department, PR department, help desk, etc. It can also be a department in a company's organizational structure, with several core members but also with some members from different departments, who work part-time or only on a specific task. Finally it can be an organization or department with only full-time members. The information you will find below is useful in any of the types of organization structures mentioned previously. The roles described here have been selected while keeping the core CERT service—incident handling—in mind. The roles can be divided into mandatory roles and optional roles."

Organization Response

Examples of Evidence Sought

- ❑ Workforce plan and supporting documentation
- ❑ Organizational chart with roles and responsibilities
- ❑ Job descriptions including required skills and abilities

- ❑ Clearance documentation
- ❑ Contractor résumés, biographies, certifications, and other supporting documentation
- ❑ Historic record of past workforce decisions
- ❑ Data collection and analysis tools or procedures for personnel or contractor performance
- ❑ Workforce planning and management tools
- ❑ Reachback or surge support SLAs or agreements

Scoring Criteria	Yes	No	Evidence
Required			
5.2.2.01 Control: A process is defined for developing and maintaining the workforce plan.	❒	❒	
5.2.2.02 Activity: A workforce plan is documented for the next one (minimum) to five (ideal) years.	❒	❒	
5.2.2.03 Activity: The workforce plan • details the number and types of personnel required (internal, external, reachback, or contractor) • accounts for required security clearances • includes contractor support criteria, required skills, certifications, reachback, and so forth • ensures there are no single points of failure for critical roles	❒	❒	
5.2.2.04 Activity: The workforce plan is fully implemented.	❒	❒	
Recommended Best Practices			
5.2.2.05 Activity: Quantitative operational statistics are analyzed and extrapolated to anticipate future staffing needs.	❒	❒	
5.2.2.06 Activity: The organization is polled for its projected needs pertaining to incident management services.	❒	❒	
5.2.2.07 Quality: The workforce plan follows organizational standards.	❒	❒	
5.2.2.08 Quality: The workforce plan is reviewed and approved by the organization's management.	❒	❒	

Institutional and Quality Improvement			
5.2.2.09 Quality: Personnel are aware of, knowledgeable of, and consistently follow the processes or procedures for this activity.	❒	❒	
5.2.2.10 Quality: A process and criteria exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	
5.2.2.11 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒
Not Applicable		❒	**Not Observed**	❒

Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement

- Include as much detail as possible in the plan, including the number and type of personnel required; contractor support criteria, staffing skills, and certifications required; and any security clearances needed.
- Develop relationships with experts in the field to provide skills if internal experts cannot be found and staff cannot be hired or trained to provide necessary specialist skills. These types of creative relationships, of course, require advance negotiation or trusted relationships between the incident management staff and the expert(s). These relationships can be defined in formal or informal agreements (with clearly defined requirements or expectations) that outline how the request for assistance is made and what restrictions are placed on any shared

information. When in-house knowledge is not sufficient, these technical specialists can be called on to fill the gap in expertise.

5.2 PROJECT/PROGRAM MANAGEMENT

5.2.3 A personnel security plan exists for incident management personnel.

Priority I

Clarification

The intent of this capability is to ensure that incident management personnel have been appropriately cleared to perform their assigned duties. This capability looks for the existence of an overarching personnel security plan that covers a range of topics, such as background checks, qualification verification, and security clearances for those involved in incident management activities. Organizations must trust the incident management personnel and be sure they have integrity and will not put themselves or the organization at risk. There are some overlaps here with the insider threat program capability 1.2.7, which also includes some aspects of employee clearances and background checks.

Team Guidance

The incident management function might be outsourced or handled by another part of the organization. In that case, this capability should be applied to that group and its activities. If the function is performed by contractors, the organization will still want to maintain control of developing and monitoring any requirements for a personnel security plan for incident management staff to ensure the plan meets organizational standards and guidance.

References

Regulatory References: None

[indirect]

FISMA Sec 3544 *Federal agency responsibilities* (a)(4) [OLRC 2003]

"(a) IN GENERAL—The head of each agency shall— […]

(3) ensure that the agency has trained personnel sufficient to assist the agency in complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines"

Guidance References:

NIST SP 800-53 Rev 4 *Security and Privacy Controls for Federal Information Systems and Organizations* [NIST 2013]

"PS-1 PERSONNEL SECURITY POLICY AND PROCEDURES

Control: The organization:

(a.) Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:

1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the personnel security policy and

associated personnel security controls; and

(b.) Reviews and updates the current:

1. Personnel security policy [Assignment: organization-defined frequency]; and
2. Personnel security procedures [Assignment: organization-defined frequency]."

Organization Response

Examples of Evidence Sought

- ❑ Documented policies and procedures on file, including
  - employee-screening policies and procedures
  - clearance requirements documentation
- ❑ Personnel clearance records for employees as well as contractors (if appropriate)
- ❑ Security clearance services and mechanisms for storing and passing clearances in compliance with organizational standards
- ❑ Repository for policies and procedures for employees to search, read, and review policy documentation

Scoring Criteria	Yes	No	Evidence
Required			
5.2.3.01 Control: Requirements exist for each relevant level of personnel security, including access to physical space, data, and computing systems, and the performance of specific activities related to incident management.	❒	❒	
5.2.3.02 Control: A comprehensive set of processes exists for a range of personnel topics, including • background checks • access control • organization-required personnel clearances	❒	❒	
5.2.3.03 Activity Personnel and organizational clearances are current and maintained as required.	❒	❒	
5.2.3.04 Activity: A personnel security program is established and followed.	❒	❒	
5.2.3.05 Activity: Personnel have been indoctrinated to security responsibilities at their • initial security briefing • annual refresher briefing	❒	❒	

Recommended Best Practices			
5.2.3.06 Activity: A pre-employment screening is conducted, and the results are filed in the organization's HR department.	❒	❒	
Institutional and Quality Improvement			
5.2.3.07 Quality: The policy and procedures for the personnel security program are reviewed at least annually and updated as needed.	❒	❒	
5.2.3.08 Quality: The policy and procedures for the personnel security program are accessible to all employees.	❒	❒	
5.2.3.09 Quality: All personnel and contractors who require clearances have been through the clearance process (or are in progress), and their clearances are up to date (e.g., background investigations have been completed with no interim clearances in force).	❒	❒	
5.2.3.10 Quality: Personnel are aware of, knowledgeable of, and consistently follow the procedures for this activity.	❒	❒	
5.2.3.11 Quality: A process and criteria exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	
5.2.3.12 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒
Not Applicable		❒	**Not Observed**	❒

Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement
• Develop a written program plan that identifies the security qualifications and clearances required for personnel. This plan should be reviewed and updated at least annually. It could be integrated into the hiring policies and practices, and could also be applied to contractors.

5.2 PROJECT/PROGRAM MANAGEMENT

5.2.4 A quality assurance (QA) program exists to ensure the quality of provided products and services.

Priority II

Clarification

The intent of this capability is to ensure the organization constantly strives to improve the quality of its incident management service via feedback mechanisms. This capability focuses on process improvement and optimization. Having a QA program in place allows the organization to gauge the success of its overall incident management function. Ensuring that all tasks are completed effectively; that resulting products and outputs are clear, timely, and accurate (e.g., advisories are always QA'd); and that personnel have the right skill sets and training to perform their job functions will result in an efficient organizational response capability. Any performance metrics and SLAs associated with key or critical services and products should be part of an overall quality program. Reviews of products and services can be continual (an inherent part of the work process), periodic, random, or a combination of these. A key aspect is the identification of necessary corrections and their implementation. Capability 5.2.6, which addresses the evaluation and improvement of the incident management function, has some overlap with this capability.

Team Guidance

This function might be outsourced or handled by another part of the organization. In that case, this capability should be applied to that group and its activities.

References

Regulatory References: None

Guidance References:

NIST SP 800-61 Rev 2 *Computer Security Incident Handling Guide* [Cichonski 2012]

> "Sec 3.4.2 Using Collected Incident Data
> [p 3-24, 3-25]
>
> Objective Assessment of Each Incident. The response to an incident that has been resolved can be analyzed to determine how effective it was.
>
> Subject Assessment of Each Incident. Incident response team members may be asked to assess their own performance, as well as that of other team members and of the entire team. Another valuable source of input is the owner of a resource that was attacked—to determine if the owner thinks the incident was handled efficiently and if the outcome was satisfactory. Besides using these metrics to measure the team's success, organizations may also find it useful to periodically audit their incident response programs. Audits will identify problems and deficiencies that can then be corrected. At a minimum, an incident response audit should evaluate the following items against applicable regulations, policies, and best practices:
>
> - Incident response policies and procedures
> - Tools and resources
> - Team model and structure
> - Incident handler training and education

- Incident documentation and reports
- The measures of success discussed earlier in this section."

Good Practice Guide for Incident Management [ENISA, 2010]

"6—Roles
For incident management to be successful, it is essential to carefully consider the roles within a CERT and to tailor these to your specific mission, constituency and environment. A CERT can be a virtual team with no formal members and with tasks distributed between different employees in various company departments such as the network operations center, internal IT security team, legal department, PR department, help desk, etc. It can also be a department in a company's organizational structure, with several core members but also with some members from different departments, who work part-time or only on a specific task. Finally it can be an organization or department with only full-time members. The information you will find below is useful in any of the types of organization structures mentioned previously. The roles described here have been selected while keeping the core CERT service—incident handling—in mind. The roles can be divided into mandatory roles and optional roles."

Organization Response

Examples of Evidence Sought

- ❑ QA program reports or other results
- ❑ QA statistics and reports
- ❑ Demonstration or observance of improvement-tracking tools and mechanisms

Scoring Criteria	Yes	No	Evidence
Required			
5.2.4.01 Control: A QA process exists.	❒	❒	
5.2.4.02 Control: Responsibility for QA is assigned.	❒	❒	
5.2.4.03 Control: Acceptable service levels and quality targets are established.	❒	❒	
5.2.4.04 Control: Defined guidance exists for reviewing products and services for quality, reporting the results, and implementing improvements.	❒	❒	
5.2.4.05 Control: Defined measures for performance, timeliness, accuracy, relevance/priority, and other quality criteria are defined and documented for each activity, product, and service and for each outsourced activity.	❒	❒	

5.2.4.06 Control: Personnel are appropriately trained about the policies and tools used to achieve and review the quality of incident management products and services.	❒	❒	
5.2.4.07 Activity: Incident management activities, products, and services are reviewed for adherence to applicable quality measures at a frequency commensurate with the product or service.	❒	❒	
5.2.4.08 Activity: QA results are used as input into improving the quality and delivery of services.	❒	❒	
5.2.4.09 Activity: Quality criteria are reviewed and adjusted periodically.	❒	❒	
Recommended Best Practices			
5.2.4.10 Control: An organizational culture of measured, managed, and constant improvement and optimization exists.	❒	❒	
5.2.4 11 Activity: Personnel are briefed at least annually on the importance of QA.	❒	❒	
Institutional and Quality Improvement			
5.2.4.12 Control: Documented procedures exist for reviewing products and services for quality, reporting the results, and implementing improvements.	❒	❒	
5.2.4.13 Quality: The QA history shows steady improvement.	❒	❒	
5.2.4.14 Quality: Personnel are aware of, knowledgeable of, and consistently follow the procedures for this activity.	❒	❒	
5.2.4.15 Quality: A process and criteria exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	
5.2.4.16 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒
Not Applicable		❒	**Not Observed**	❒

Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement

- Build in a process to perform QA reviews or tests on a periodic (e.g., annual) and consistent basis, and use the results to improve the operation of the incident management function. Implementing a QA program successfully means that personnel know and understand management's commitment to quality and understand their role in ensuring it.
- Perform the following types of actions: training and mentoring in a quality culture; sharing lessons learned from quality reviews; and rewarding high-quality behavior. All these actions can improve the incident management culture within an organization and, in turn, improve the quality of incident management services.

5.2 PROJECT/PROGRAM MANAGEMENT

5.2.5 An established plan exists to ensure continuity of operations for incident management.

Priority I

Clarification

The intent of this capability is to ensure the continuity of operations (COOP) for incident management activities. This includes recovery, reconstitution, and restoration of incident management data systems, and services. Just like other organizational units, the incident management function must be able to continue operations during any type of outage or disruption, even when under attack. Security and IT best practices recommend a written business resumption plan that includes

- a backup site where operations can move if the primary physical location becomes unusable
- backed-up and mirrored services such as DNS, email, web services, and other communication support that are needed for daily or crisis operations
- support for network monitoring and incident tracking
- the designation of a COOP site

Although most organizations have an enterprise COOP plan, it does not always include the incident management activities and responsibilities. In those cases, a separate incident management plan should be developed that integrates with the overall organizational COOP plan. Any existing incident management, business resumption, COOP, or disaster recovery plans must align with the version detailing the organizational enterprise activities.

Team Guidance

Note that the terms *business resumption*, *COOP*, *disaster recovery*, and *emergency response* are often used interchangeably. One of these plans may exist and cover all aspects, or several plans may exist to address multiple types of situations. The assessment team needs to ask these questions carefully to determine the scope of the existing plans and how they are used to support the incident management function.

To meet this capability, the plans can stand alone or be part of the organizational enterprise plans.

References

Regulatory References:

FISMA Sec 3544 *Federal agency responsibilities* (b)(8) [OLRC 2003]

> "(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] to provide information security for the information and information systems that support the operations and assets of the agency […] that includes—
>
> (8) plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency."

Guidance References: None

[indirect]

NIST SP 800-34 Rev 1 *Contingency Planning Guide for Federal Information Systems* [Swanson 2010]

> "This publication assists organizations in understanding the purpose, process, and format of ISCP (Information System Contingency Plan) development through practical, real-world guidelines. While the principles establish a baseline to meet most organizational needs, it is recognized that each organization may have additional requirements specific to its own operating environment. This guidance document provides background information on interrelationships between information system contingency planning and other types of security and emergency management-related contingency plans, organizational resiliency, and the system development lifecycle (SDLC). The document provides guidance to help personnel evaluate information systems and operations to determine contingency planning (CP) requirements and priorities."

A Step-By-Step Approach on How to Set Up a CSIRT [ENISA, 2006]

> "A.2 CSIRT Services
> Business Continuity and Disaster Recovery Planning
> Based on past occurrences and future predictions of emerging incident or security trends, more and more incidents have the potential to result in serious degradation of business operations. Therefore, planning efforts should consider CSIRT experience and recommendations in determining how best to respond to such incidents to ensure the continuity of business operations. CSIRTs performing this service are involved in business continuity and disaster recovery planning for events related to computer security threats and attacks."

Organization Response

Examples of Evidence Sought

- ❑ A plan that addresses incident management COOP such as a
  - business resumption plan
  - contingency plan
  - disaster recovery plan
  - emergency response plan
- ❑ Plan for moving primary operations (e.g., personnel, computing infrastructure, email, phone) to a COOP site, when necessary
- ❑ List of incident management functions and services that are critical to operate during disasters or emergencies
- ❑ List of incident management roles and responsibilities that must continue to operate during disasters and emergencies

Scoring Criteria	Yes	No	Evidence
Required			
5.2.5.01 Control: Mission-critical incident management services, systems, personnel, and equipment are identified and documented.	❒	❒	
5.2.5.02 Control: Acceptable service levels for recovery, reconstitution, and restoration activities have been identified and agreed to by organizational management.	❒	❒	
5.2.5.03 Activity: A disaster recovery plan is documented and approved.	❒	❒	
5.2.5.04 Activity: A backup site or COOP site is established and maintained and meets the requirements of the DR plan.	❒	❒	
5.2.5.05 Activity: Resources for mirrored services are established and kept up to date.	❒	❒	
5.2.5.06 Activity: Scenario-based exercises are conducted at least annually to test contingency, service resumption, disaster recovery, emergency response, and other plans.	❒	❒	
5.2.5.07 Quality: Plans are updated and reviewed at least annually.	❒	❒	
Recommended Best Practices			
None.	❒	❒	
Institutional and Quality Improvement			
5.2.5.08 Quality: Personnel are aware of, knowledgeable of, and consistently follow the procedures for this activity.	❒	❒	
5.2.5.09 Quality: A process and criteria exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	
5.2.5.10 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	Met (all Required indicators have Yes answers)	❒	Not Met (one or more Required indicators have a No answer)	❒
Not Applicable		❒	Not Observed	❒

Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement

- Ensure that these plans can be accessed easily and incident management personnel know how to initiate and follow them.
- Ensure that these plans provide for personnel safety first in the event of a disaster.
- Integrate these plans with any other organizational disaster recovery and business resumption plans.
- Re-evaluate these plans when organizational changes occur, such as reorganizations, mergers, and acquisitions.

5.2 PROJECT/PROGRAM MANAGEMENT

5.2.6 The effectiveness of the incident management function in meeting its mission is routinely evaluated and improved.

Priority III

Clarification

The intent of this capability is to ensure that the performance of the IM function is monitored for effectiveness and improvements are made whenever deficiencies are found. In order to do this, criteria for what constitutes effectiveness for the IM function need to be defined. The effectiveness of the IM function will be related to the mission, objectives, and provided services of the IM function. For example, effectiveness may be measured by the efficiency of incident response or the satisfaction of the recipients of alerts and notifications.

The measures that indicate whether those effectiveness criteria are being met are used to periodically evaluate the IM function. This does not mean there must be a continuous monitoring of all these measures. It is up to the organization to determine how best to evaluate the effectiveness of the IM function and the desired frequency for evaluation (e.g., yearly). Some critical aspects may need more frequent, and preferably automated, evaluation. For example, monitoring the percentage of closed versus open incidents might be more critical to know than the number of media calls that are handled.

When deficiencies are found, an improvement plan needs to be developed and improvements made. Measuring the impact of those improvements to ensure improvement has occurred is also essential. The deficiencies, recommendations, and improvements will likely need to be reported to and coordinated with stakeholders, including senior management, for the IM function. Note that evaluation of the IM function may be an internal or external process.

Team Guidance

The team should look for the existence of a measurement and improvement program, including what aspects of the IM function are considered critical, the associated criteria for effectiveness, measures to be collected, the frequency of measurement collection, how the measurement data is analyzed, and the process for making and verifying improvements. This type of activity can be associated with a broader process improvement or performance measurement program for the organization; it may not be specific to the incident management function and may therefore be performed by a different group. If that is the case, the other group should be assessed against this capability.

References

Regulatory References: None

Guidance References: None

Agency Response

Examples of Evidence Sought			
❑ Plan for measuring and evaluating the incident management function ❑ Samples of measurement data collected ❑ Analysis reports of collected measurement data ❑ Samples of improvement plans to correct deficiencies or weaknesses			
Scoring Criteria	Yes	No	Evidence
Required			
5.2.6.01 Control: Critical aspects of the IM function that need to be evaluated for effectiveness have been identified.	❒	❒	
5.2.6.02 Control: Criteria are defined for what constitutes effectiveness for critical aspects of the IM function.	❒	❒	
5.2.6.03 Activity: A plan for evaluating the effectiveness of the incident management function is developed and maintained.	❒	❒	
5.2.6.04 Activity: A process for evaluating the effectiveness of the incident management function is defined.	❒	❒	
5.2.6.05 Activity: Deficiencies in the incident management function are identified.	❒	❒	
5.2.6.06 Activity: Improvement plans are developed and implemented for identified deficiencies.	❒	❒	
5.2.6.07 Activity: Improvements are evaluated to ensure the desired results have been achieved.	❒	❒	
Recommended Best Practices			
5.2.6.08 Activity: Automated data collection is used where possible.	❒	❒	
5.2.6.09 Activity: Improvements are coordinated with any broader organization-wide improvement programs to gain efficiencies.	❒	❒	

Institutional and Quality Improvement			
5.2.6.10 Quality: Personnel are aware of, knowledgeable of, and consistently perform the procedures, processes, methodologies, and technologies for performing this activity.	❒	❒	

Scoring	Met (all Required indicators have Yes answers)	❒	Not Met (one or more Required indicators have a No answer)	❒
Not Applicable		❒	Not Observed	❒

Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement
None

5.3 IM TECHNOLOGY DEVELOPMENT, EVALUATION, AND IMPLEMENTATION

5.3.1 The incident management function has the tools it needs to meet its mission.

Priority I

Clarification

The intent of this capability is to ensure that the incident management function has the tools it needs to meet its mission. As used in this capability, the term *tools* refers to the software and hardware used to support incident management activities and other provided services such as

- an incident reporting system or workflow management system for documenting and tracking incidents
- databases and data repositories for storing incident management information
- mechanisms or applications for secure email, voice communication, and data transfer
- mechanisms and tools for incident analysis and correlation

Tools may be commercial or open source depending on the requirements (or budget constraints) of the parent organization. Some organizations do not allow use of open source tools. Tools may be acquired externally or developed in-house.

Different components of the incident management function may require different tools based on their role and responsibilities.

To ensure that the organization has the right tools for incident management, a process for identifying needed tools and determining their requirements for implementation should be in place. This process could follow the normal software acquisition lifecycle or some other organization-specific process.

The lifecycle for acquiring and developing tools to support an incident management function comprises the following core activities:

- Establish requirements for tools.
- Acquire or develop tools that meet these requirements.
- Test tools within the incident management environment.
- Deploy tools for operational use.
- Operate and sustain tools over time.

This capability is focused specifically on (1) establishing and documenting requirements for tools and (2) acquiring or developing tools that meet those requirements. Testing and deploying tools are addressed in capability 5.3.2.

Requirements for a tool should include the purpose or proposed use of the tool; specifications for software and hardware; documentation for operating, using, and sustaining the tool; and specification for interfaces with other tools. Formal documentation of agreements with vendors, such as contracts or purchase orders, should specify the versions of any software and hardware being used.

Capability 5.3.3, which focuses on keeping up with emerging technologies, also ties into this capability. The incident management function needs to stay abreast of any new tools available to improve incident handling processes and tasks.

Team Guidance

The team should look for evidence that the IM function has a process in place to evaluate and identify what type of tools it needs to meet its mission and a corresponding process for acquiring and deploying those tools. This process may be formal or informal.

If a formal process is followed, the team should be able to examine requirements documents for the suite of tools currently deployed in the incident management environment. The team should also be able to examine all policies, processes, and procedures related to acquiring and developing new tools. These policies, processes, and procedures should indicate the specific approach employed for acquiring tools from vendors and developing tools in-house (if applicable).

If the process is informal, and no supporting documentation exists, the team will need to observe a demonstration of how tools are identified for acquisition and deployment.

References

Regulatory References: None

Guidance References:

NIST 800-61 Rev. 2 *Computer Security Incident Handling Guide* [Cichonski 2012]

> Sec 3.1.1 "Preparing to Handle Incidents
>
> The lists below provide examples of tools and resources available that may be of value during incident handling. These lists are intended to be a starting point for discussions about which tools and resources an organization's incident handlers need."

Good Practice Guide for Incident Management [ENISA, 2010]

> "8.9 Tools
> 8.9.1 Clearing House for Incident Handling Tools (CHIHT)
> Within Task Force CSIRT organized by TERENA in 2000, the idea of collecting valuable CERT tools and guidelines was developed. Thanks to this initiative, a collection of tools used by various European CERTs now exists. The project is called 'Clearing House for Incident Handling Tools'. It has the unique value of providing information not only about the tools but also about those who are using them. So, if you want to choose tools to use in your team, you can ask for opinions from other CERTs. You can also ask these teams for support. […]
> 8.9.2 Incident handling systems
> Incident handling systems comprise a special group of tools. […]"

Agency Response

Examples of Evidence Sought

- ❑ Requirements documents for tools
- ❑ Policies for acquiring or developing tools
- ❑ Processes and procedures for acquiring or developing tools
- ❑ Contracts and purchase orders for tools
- ❑ Software licenses

Scoring Criteria	Yes	No	Evidence
Required			
5.3.1.01 Control: Documented guidance exists for defining tool requirements and acquiring, developing, deploying, and maintaining tools.	❒	❒	
5.3.1.02 Activity: Requirements for tools are established and documented.	❒	❒	
5.3.1.03 Activity: Tools that are adequate to meet requirements are acquired and maintained.	❒	❒	
5.3.1.04 Activity: Licenses for all tools are kept up to date.	❒	❒	
Recommended Best Practices			
None			
Institutional and Quality Improvement			
5.3.1.05 Control: Documented procedures exist for defining tool requirements and acquiring, developing, deploying, and maintaining tools.	❒	❒	
5.3.1.06 Quality: Personnel have a technical understanding and knowledge of the software, tools, databases, and so forth that support incident management activities.	❒	❒	
5.3.1.07 Quality: Personnel responsible for tool acquisition or development are aware of, knowledgeable of, and consistently follow the procedures for this activity.	❒	❒	
5.3.1.08 Quality: A process and criteria exist for evaluating and improving the quality of this activity.	❒	❒	
5.3.1.09 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒
Not Applicable		❒	**Not Observed**	❒

Evidence Collected					
Document Review		Interviews		Direct Observation	
Notes					
Suggestions for Improvement					
None					

5.3 IM TECHNOLOGY DEVELOPMENT, EVALUATION, AND IMPLEMENTATION

5.3.2 Software tools are tested for use within the incident management environment.

Priority II

Clarification

The intent of this capability is to ensure that there is a testbed capability to safely evaluate tools. The focus is on validating and verifying the safety of the tools, technology, software, and hardware used to support incident management activities (including sensors; tools for data analysis, handling and tracking events and incidents, and detecting malicious code; IDSs; IPSs; firewalls; routers; system upgrades, etc.) and making sure they do not introduce vulnerabilities into the environment. Before being deployed, tools must be tested to ensure that they perform as expected and do not interact in unexpected ways with existing software, hardware, and applications.

Team Guidance

The team should look for evidence that all tools (software or hardware, new OS versions, etc.) are tested prior to being installed and/or implemented in production network(s). The team should be able to verify the existence of a testbed capability and records of its use. Records or indications should also exist that the tools currently in the incident management environment were tested in the testbed prior to deployment. Testing and deployment procedures for new tools should indicate the requirement to safely test in the testbed prior to release.

References

Regulatory References: None

Guidance References: None

[indirect]

NIST SP 800-128 *Guide for Security-Focused Configuration Management of Information Systems* [Johnson 2011]

> "Chapter 3: Establish Configuration Test Environment and Program
>
> Some organizations may wish to establish and maintain a configuration test environment and program for testing IT products, tools, and proposed changes to them in a centrally managed environment isolated from the production environment. The test environment is used for various types of testing to include:
>
> - IT products proposed for approval and use within the organization;
> - Configuration settings for approved IT products;
> - Patches issued by suppliers prior to their rollout through the organization;
> - Validation of tools that detect unapproved configuration settings;
> - Verification of testing processes to validate approved configuration settings;
> - Security impact analyses; and

- Other configuration-related changes."

NIST SP 800-61 Rev 2 *Computer Security Incident Handling Guide* [Cichonski 2012]

"Sec 3.1.1 Preparing to Handle Incidents

Tools and Resources for Incident Handlers
Incident Analysis Hardware and Software: "Digital forensic workstations and/or backup devices; Laptops; Spare workstations, servers, and networking equipment, or the virtualized equivalents; Blank removable media; Portable printer; Packet sniffers and protocol analyzers; Digital forensic software; Removable media; Evidence gathering accessories."

Organization Response

Examples of Evidence Sought

- ❑ List of tools that have been tested and are allowed to be used in production networks
- ❑ Documented test results of products assessed in the testbed environment
- ❑ Policies requiring testing prior to release
- ❑ Testbed description or operations procedures
- ❑ Procedures for testing and deploying new tools into the incident management environment
- ❑ System and procedures for the configuration and/or change management of software and tools
- ❑ System and procedures for the patch management of software and tools
- ❑ QA audit results of software and tool testing and deployment

Scoring Criteria	Yes	No	Evidence
Required			
5.3.2.01 Control: Guidelines exist that explain how the tools should be evaluated and tested to support incident management activities.	❒	❒	
5.3.2.02 Control: Documented guidance exists for obtaining, testing, and deploying tools within the incident management environment.	❒	❒	
5.3.2.03 Activity: Trusted or tested suites of tools are used to perform incident management activities.	❒	❒	
5.3.2.04 Activity: New tools are tested to ensure they will not disrupt operations.	❒	❒	
5.3.2.05 Activity: New tools are tested to ensure they function as advertised and expected.	❒	❒	

Recommended Best Practices			
5.3.2.06 Control: An isolated (nonproduction) network exists for testing tools, new software/hardware, and other technology prior to their deployment on the production network.	❒	❒	
Institutional and Quality Improvement			
5.3.2.07 Control: Documented procedures exist for obtaining, testing, and deploying tools within the incident management environment.	❒	❒	
5.3.2.08 Control: A documented process exists for reviewing the performance and usefulness of software tools (e.g., sensor data analysis, incident/event handling, and malicious code detection).	❒	❒	
5.3.2.09 Quality: Personnel have a technical understanding and knowledge of the software, tools, databases, and so forth that support incident management activities.	❒	❒	
5.3.2.10 Quality: Personnel are aware of, knowledgeable of, and consistently follow the procedures for this activity.	❒	❒	
5.3.2.11 Quality: A process and criteria exist (including those defining adequate testing of incident management tools) for evaluating and improving the quality of this activity.	❒	❒	
5.3.2.12 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒
Not Applicable		❒	**Not Observed**	❒

Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement
• Create plans for developing a resource for testing new software/hardware, tools, equipment, etc. • Develop and document a formalized process for evaluating new software, technologies, etc. • Create a plan for developing formal procedures, guidelines, and best practices for testing software used in the incident management environment.

5.3 IM TECHNOLOGY DEVELOPMENT, EVALUATION, AND IMPLEMENTATION

5.3.3 The IT infrastructure for incident management is adequate to support incident management operations.

Priority I

Clarification

The intent of this capability is to ensure incident management personnel have the IT infrastructure they need to support their tasks. All organizations require the right infrastructure when managing incidents. Without the appropriate tools, technologies, and security defenses, incident management personnel cannot meet the expectations of the organization they serve. The incident management infrastructure includes

- the physical location and security of incident management staff and data
- staff office and home equipment such as telephones, desktops, laptops, projectors, shredding machines, whiteboards, cell phones, pagers, and so forth
- incident management networks, systems, and internal/external defenses such as routers, firewalls, and IDSs
- incident management tools and applications to support incident handling and other provided services such as
  - databases, data repositories, and data analysis tools for storing incident management information
  - mechanisms or applications for secure email, voice communications, and data transfer
  - mechanisms for incident analysis and correlation

When a specifically designated CSIRT exists, the IT infrastructure for incident management may be separate from the organization's general infrastructure. However, some ad hoc or smaller teams use the organization's general infrastructure for their work and might only have a small collection of special tools or equipment.

Incident management facilities and the network and telecommunications infrastructures must be designed with great care to protect the sensitive data collected from them.

Team Guidance

The infrastructure used for incident management activities might be the same one used by the organization (i.e., it might not be separate). In that case, the team must look at the organization's infrastructure that applies to incident management functions.

References

Regulatory References: None

Guidance References: None

[indirect]

NIST SP 800-37 Rev 1 *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Lifecycle Approach* [NIST 2010]

> "The purpose of this publication is to provide guidelines for applying the Risk Management Framework to Federal information systems to include conducting the activities of security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring."

NIST SP 800-61 Rev 2 *Computer Security Incident Handling Guide* [Cichonski 2012]

> "Sec 3.1.1 Preparing to Handle Incidents
>
> Tools and Resources for Incident Handlers
> The lists below provide examples of tools and resources available that may be of value during incident handling. These lists are intended to be a starting point for discussions about which tools and resources an organization's incident handlers need."

Organization Response

Examples of Evidence Sought

- ❑ Long-term strategic development plan or upgrade plan for infrastructure
- ❑ Inventory of IT infrastructure components
- ❑ Hardware/software license documentation
- ❑ Hardware/software lifecycle plan
- ❑ Observation of configuration management mechanisms
- ❑ Documentation of the testing results of recent operations
- ❑ Up-to-date technical reference library
- ❑ Equipment acquisition process
- ❑ Certification and accreditation plan
- ❑ Hardware/software lifecycle and configuration management mechanism

Scoring Criteria	Yes	No	Evidence
Required			
5.3.3.01 Control: A process exists for determining, documenting, submitting, and authorizing improvements to the IT infrastructure for incident management (as either a separate process or part of normal organizational processes).	❒	❒	
5.3.3.02 Activity: Incident management personnel or management identify their own IT infrastructure requirements.	❒	❒	
5.3.3.03 Activity: There is an IT infrastructure budget for incident management.	❒	❒	

5.3.3.04 Activity: The necessary incident management infrastructure is acquired and managed.	❒	❒	
5.3.3.05 Activity: Improvements and upgrades are identified, planned, requested, acquired, and implemented.	❒	❒	
5.3.3.06 Activity: Change and configuration management processes are followed when making changes to the incident management infrastructure.	❒	❒	
5.3.3.07 Quality: The adequacy of the incident management IT infrastructure is reviewed at least annually, and improvements are requested.	❒	❒	
5.3.3.08 Quality: All equipment certifications and accreditations are up to date.	❒	❒	
Recommended Best Practices			
5.3.3.09 Activity: Funding is allocated for improving and sustaining operations such as equipment, technical materials, security publications, and professional training.	❒	❒	
5.3.3.10 Quality: The hardware and software inventory is up to date and accurate.	❒	❒	
5.3.3.11 Quality: All licensing is up to date and accurate.	❒	❒	
5.3.3.12 Quality: Configuration management is reviewed independently and assessed at least annually.	❒	❒	
Institutional and Quality Improvement			
5.3.3.13 Quality: Personnel are familiar with and adhere to the lifecycle and configuration management plan.	❒	❒	
5.3.3.14 Quality: Personnel are aware of, knowledgeable of, and consistently follow the procedures for this activity.	❒	❒	
5.3.3.15 Quality: A process and criteria exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	
5.3.3.16 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	Met (all Required indicators have Yes answers)	❒	Not Met (one or more Required indicators have a No answer)	❒
Not Applicable		❒	Not Observed	❒

Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement

- Develop an infrastructure and corresponding funding plan to ensure
  - incident management personnel have the tools they need
  - people and data are adequately protected
  - the ability to plan for future growth and updates is realized
- Employ a certification and accreditation program for all systems and networks used by incident management personnel.
- Follow the best practices for security, regarding patch and configuration management.
- Establish the appropriate internal and external defenses such as firewalls, an IDS, routers, and network monitoring for the incident management infrastructure.
- Look for economies of scale in purchasing.
- Keep any licenses for software and hardware up to date.

5.4 PERSONNEL

5.4.1 A training program exists for incident management personnel. Priority I

Clarification

The intent of this capability is to ensure that incident management personnel participate in appropriate training activities to build the knowledge, skills, and abilities they need to perform their roles successfully. This capability focuses on the need to establish a training program for incident management personnel (for new staff as well as existing staff). To be successful, personnel must have the requisite knowledge, skills, and abilities to perform their tasks in support of their mission and goals, and the organization being served. In addition, incident management personnel must understand their working environment and be able to use the tools that support their assigned, incident management roles and responsibilities.

A robust training program should address a broad range of activities for building staff members' knowledge, skills and abilities, including

- assessing an individual's current competencies and his or her ability to apply those competencies when performing specific tasks
- developing a training plan, or a course of action, intended to maintain or improve an individual's competencies (note that such a plan may also be part of a professional development plan, as described in 5.2.3)
- acquiring the knowledge, skills, and abilities required to maintain or improve an individual's competencies
- validating whether an individual's training actions have addressed his or her competency needs
- testing an individual's readiness to perform a specific task as required

The training program should be based on a set of criteria that establish the scope of ETA requirements and minimum competency levels for incident management activities. This program should include new employee orientation, required ETA, and refresher training for existing staff. In addition, successful training programs must provide the organizational structure and support needed to ensure that individuals are ready to apply the knowledge, skills, and abilities they need to perform their incident management tasks. Such structure and support could include management sponsorship, funding, opportunity and time to pursue training, readily available sources for training, and ease of requesting training.

ETA requirements and minimum competency levels work best when aligned with a role. Ideally, requirements for a role should include both task-specific and enabling competencies. In this context, task-specific competencies are the subset of knowledge, skills, and abilities that directly affect the ability to perform a task. For example, a task-specific competency for a cybersecurity analyst would be the ability to use specific tools, such as intrusion detection tools. In contrast, enabling competencies indirectly support the completion of a task. For example, the cybersecurity analyst needs to communicate information about possible security incidents with his or her colleagues.

Team Guidance

The team should look for evidence that a training program exists for incident management personnel. The training program must address security policies and other IT-related security topics, such as physical, personnel, and OPSEC. It must incorporate established ETA requirements, standards, and minimum competency levels, and be in compliance with regulations and requirements.

The team should also look for evidence that the ETA requirements and minimum competency levels for incident management activities have been developed and documented. The team should look for evidence that ETA requirements include both task-specific and enabling knowledge, skills, and abilities.

References

Regulatory References: None

[indirect]

FISMA Sec 3544 *Federal agency responsibilities* (a)(3)(D) and (a)(4) [OLRC 2003]

> "(a) IN GENERAL—The head of each agency shall— […]
>
> (3) delegate to the agency Chief Information Officer established under section 3506 (or comparable official in an agency not covered by such section) the authority to ensure compliance with the requirements imposed on the agency under this subchapter, including— […]
>
> (C) training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities; […]
>
> (4) ensure that the agency has trained personnel sufficient to assist the agency in complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines"

Guidance References:

NIST SP 800-53 Rev 4 *Security and Privacy Controls for Federal Information Systems and Organizations* [NIST 2013]

> "IR-2 INCIDENT RESPONSE TRAINING
>
> **Control:** The organization provides incident response training to information system users consistent with assigned roles and responsibilities:
>
> (a.) Within [*Assignment: organization-defined time period*] of assuming an incident response role or responsibility;
>
> (b.) When required by information system changes; […]"

[indirect]

NIST SP 800-61 Rev 2 *Computer Security Incident Handling Guide* [Cichonski 2012]

> "Sec 2.4.3 Incident Response Personnel
> [p 2-13]
>
> Members of the incident response team should have excellent technical skills […] Every team member should have good problem solving skills […] It is important to counteract staff burnout by providing opportunities for learning and growth. […] Incident response team members should have other skills in addition to technical expertise. Teamwork skills […] good communication skills. Speaking skills […] Writing skills [...]"

Good Practice Guide for Incident Management [ENISA, 2010]

"Sec 9.2.2 Staff training
People will never stop learning. People also want to be trained on the job, and use their job to widen and deepen their skills and work on their personal development. As a CERT, you need to keep investing in your people to widen the skills of your staff in order to foster their personal development and nurture the skills in the team. This will keep the overall skill-set of the CERT up-to-date with fast developing technologies and trends in attacks. […]"

Agency Response

Examples of Evidence Sought

- ❑ List(s) of recommendations and information resources on training topics, courses, conferences, and so forth that personnel can select from
- ❑ Job descriptions listing required skills and knowledge
- ❑ Training records on file
- ❑ Documented competencies for incident management roles or activities
- ❑ Documented goals for technical training for incident management personnel
- ❑ Demonstration that personnel have the knowledge, skills, and abilities needed to perform their technical work (e.g., they can explain what training they received and show how they use the tools, analyze logs, and access databases)
- ❑ Mechanism to validate that training is completed, tracked, and recorded for each employee's training requirements, and that qualifications and deficiencies are noted (e.g., test results, certificates, records of CBT access, tracking databases, or spreadsheets)
- ❑ Online training available through CDs or intranet, online training opportunities, local/classroom environments, and so forth

Scoring Criteria	Yes	No	Evidence
Required			
5.4.1.01 Control: ETA requirements for incident management personnel are defined and documented.	❒	❒	
5.4.1.02 Control: Training policy or guidance states that training activities are required for incident management personnel.	❒	❒	
5.4.1.03 Control: Security policies and other IT-related issues (e.g., physical, personnel, OPSEC) are covered.	❒	❒	
5.4.1.04 Activity: Minimum competency levels for incident management personnel are defined and documented.	❒	❒	

5.4.1.05 Activity: All incident management personnel attend initial IT security and awareness training, as well as other relevant incident management training courses (e.g., training that addresses incident management roles and responsibilities).	❒	❒	
5.4.1.06 Activity: Training for incident management personnel includes simulated events to facilitate effective response by personnel in normal IM operations and crisis situations.	❒	❒	
5.4.1.07 Activity: Incident management personnel periodically (at least annually) identify training activities (e.g., training, mentoring, self-study) and document them in individual training plans.	❒	❒	
5.4.1.08 Activity: Incident management personnel acquire needed knowledge, skills, and abilities that fully meet their individual training plan.	❒	❒	
5.4.1.09 Activity: Training records and histories for IM personnel are documented and maintained.	❒	❒	
Recommended Best Practices			
5.4.1.10 Control: Documented policies exist that require the establishment of ETA requirements and minimum competency levels (type, frequency, etc.).	❒	❒	
5.4.1.11 Control: Documented policies describe the training program for incident management personnel.	❒	❒	
5.4.1.12 Activity: ETA requirements and minimum competency levels are updated at least annually.	❒	❒	
5.4.1.13 Activity: Automated mechanisms are used to provide a more thorough and realistic training environment.	❒	❒	
5.4.1.14 Activity: Annual refreshers for security awareness and other relevant training are provided.	❒	❒	
5.4.1.15 Activity: Funding is allocated for external technical training for all incident management personnel. (This might include contracted employees when such training is not covered in the contract.)	❒	❒	
5.4.1.16 Activity: The competencies (i.e., knowledge, skills, and abilities) that incident management personnel must have to meet the needs for their roles are formally assessed and baselined.	❒	❒	

5.4.1.17 Activity: The extent to which incident management personnel have acquire the desired knowledge, skills, and abilities through their training activities is formally validated.	❒	❒	
5.4.1.18 Activity: Incident management personnel's readiness to perform tasks in a real-world setting is tested.	❒	❒	
Institutional and Quality Improvement			
5.4.1.19 Control: Documented procedures exist that define how to establish and maintain the ETA requirements and minimum competency levels (type, frequency, etc.).	❒	❒	
5.4.1.20 Control: Documented procedures exist that describe the training program for incident management personnel.	❒	❒	
5.4.1.21 Quality: Personnel are knowledgeable and aware of their training requirements and minimum competency levels and work with management to obtain any needed ETA.	❒	❒	
5.4.1.22 Quality: A process and criteria exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	
5.4.1.23 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒	
Not Applicable		❒	**Not Observed**	❒	
Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement
• Develop matrices for all roles and responsibilities involved in incident management and determine the range of knowledge, skills, and abilities needed to effectively perform these activities. • Determine the requirements for appropriate levels for certifications or other professional degrees including proficiency in a specific technology or capability. Offer employees incentives such as bonuses or promotions for developing professional knowledge, skills, and abilities.

5.4 PERSONNEL

5.4.2 Support for professional development exists for incident management personnel.

Priority III

Clarification

The intent of this capability is to support the continued, professional development of incident management personnel. A formal program may not exist, but support for professional and career development is required. It is important to note that different approaches and levels of support might exist for organization and contractor personnel. For this capability to be performed effectively, all personnel performing incident management functions should have professional and career development options. Establishing an approach for developing a career or growth path will help ensure personnel remain committed to the work and have a way to increase their knowledge and skills. In addition, exposing personnel to other information assurance (IA) or IM training will increase their awareness of security-related issues.

Part of professional development is staying current with changes in the security and incident management field; along with staying current with the environment in which they and their organization work. It is important to be aware of new types of tools and mitigation strategies that could be used by the incident management team or the organization. They also need to stay current with new threats to or vulnerabilities in any software and hardware used by their organization. As emerging technologies are incorporated into the organization's infrastructure, incident management personnel need to become knowledgeable about how the technology works. They need to know special considerations for how this technology is implemented or integrated with other systems or networks, and any information that may indicate potential threats and problems.

The danger in not keeping abreast of new or emerging technologies that may be incorporated into the organization's systems is that when incidents, attacks, and threats occur, the incident management activities may fail to properly handle the situations. That failure can threaten the organization's assets and its ability to continue to do business. Note that this is different from capability 3.3.1 for situational awareness because it focuses only on emerging technologies.

Incident management staff can stay current with emerging technologies through various means including but not limiting to

- reviewing information extracted from open source monitoring
- attending vendor training or focused security training
- attending conferences or workshops
- reading general security publications
- participating in or joining professional associations such as the Institute of Electrical and Electronics Engineers (IEEE); the Association for Computing Machinery (ACM); Information Systems Audit and Control Association (ISACA); and InfraGard, a partnership between the FBI and the private sector; or other similar organizations
- information sharing with others in their field, such as technical exchanges or workshops

They should communicate with other parties who are authorities in these fields to ensure they get the most accurate information or interpretation.

Team Guidance

The team should look for evidence that support for professional and career development exists for incident management personnel. The team should review documented policies and procedures that delineate how personnel participate in professional development activities and look at data that tracks that participation.

The team should look for

- evidence that IM personnel regularly pursue activities to stay current with new and emerging computing technologies, new vulnerabilities in those technologies, and new tools and mitigation strategies for preventing and responding to threats and incidents
- documentation or training plans that require this activity, such as policies, documented procedures, KSAs, or assigned responsibilities
- training records showing attendance at relevant workshops or conferences
- membership subscriptions to professional associations
- publications or reports that have been read by staff which pertain to emerging technologies and tools

Some organizations may have comprehensive training plans that include requirements for keeping up with emerging technologies or maintaining contacts and memberships in security groups or associations.

The capability to stay abreast of emerging technologies might be outsourced or handled by another part of the organization. In that case, indicators specific to staying abreast of emerging technology should be applied to that group and its activities. However, the team should make sure that any information gather by any other group is shared with the incident management staff.

References

Regulatory References: None

[indirect]

FISMA Sec 3544 *Federal agency responsibilities* (a)(3)(D) and (a)(4) [OLRC 2003]

> "(a) IN GENERAL—The head of each agency shall— […]
>
> (3) delegate to the agency Chief Information Officer established under Section 3506 (or comparable official in an agency not covered by such section) the authority to ensure compliance with the requirements imposed on the agency under this subchapter, including— […]
>
> (D) training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities; […]
>
> (4) ensure that the agency has trained personnel sufficient to assist the agency in complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines"

Guidance References:

NIST SP 800-61 Rev 2 *Computer Security Incident Handling Guide* [Cichonski 2012]

> "Sec 2.4.3 Incident Response Personnel
>
> It is important to counteract staff burnout by providing opportunities for learning and growth."

Organization Response

Examples of Evidence Sought
❑ Schedule for appropriate technology or IA forums for planned participation ❑ Mechanisms for requesting and authorizing participation in such events or other professional development events ❑ Material received at forums (presentations, documents, handouts, CDs, other media) ❑ Examples of forms to request professional development ❑ Database for tracking professional activities for personnel/team accomplishments ❑ Organization-owned and centrally managed IA/IM training and documentation reference library for training material ❑ Documented responsibilities for maintaining awareness of emerging technologies ❑ Documented training and education plans that include maintaining awareness of emerging technologies and contact with security groups and associations ❑ Product evaluation reports on file ❑ Records of information gathered ❑ Archives of emails from mailing-list subscriptions ❑ Records of periodic vendor product demonstrations or technologies on-site ❑ Technology periodicals or other resource media ❑ RSS or other types of newsfeeds with targeted information ❑ Records of attending conferences or workshops or other professional development activities ❑ Copies of subscriptions or memberships in professional associations ❑ Observing staff collecting information or attending training on emerging technologies

Scoring Criteria	Yes	No	Evidence
Required			
5.4.2.01 Control: Participation in professional development activities is a documented goal for the organization and, as applicable, contractor personnel.	❒	❒	
5.4.2.02 Control: Documented guidance exists that delineates how personnel participate in professional development activities.	❒	❒	
5.4.2.03 Activity: Information on emerging technologies, related vulnerabilities, tools, and mitigation strategies is collected.	❒	❒	

5.4.2.04 Activity: Personnel share information/resources with colleagues and incident management staff to raise awareness within the team.	❒	❒	
5.4.2.05 Activity: Personnel participate in professional development activities.	❒	❒	
5.4.2.06 Activity: Participation in professional development activities is tracked.	❒	❒	
Recommended Best Practices			
5.4.2.07 Control: Guidelines exist that explain the professional development support that is provided.	❒	❒	
5.4.2.08 Control: A tracking system exists for the use of professional development materials available to or collected by incident management personnel.	❒	❒	
5.4.2.09 Activity: Funding is allocated for purchasing the latest, relevant technical books, research publications, and materials for staff.	❒	❒	
5.4.2.10 Activity: An annual (or other interim) review of professional development activities is performed.	❒	❒	
5.4.2.11 Activity: Personnel communicate with the organization's personnel and management to discuss emerging technologies and impacts within the organization.	❒	❒	
5.4.2.12 Activity: Impacts identified by reviewing and understanding emerging technologies is contributed to the change management review process when implementing new hardware, software, or processes.	❒	❒	
5.4.2.13 Activity: Collected information is stored in a knowledge management system so it can be tagged and easily searched or accessed by incident management personnel.	❒	❒	
Institutional and Quality Improvement			
5.4.2.14 Control: Documented guidance detail approved methods for staff to stay abreast of emerging technologies, and corresponding vulnerabilities, tools, and mitigation strategies.	❒	❒	
5.4.2.15 Control: Documented procedures exist that describe how personnel participate in professional development activities.	❒	❒	

5.4.2.16 Quality: Personnel are aware of, knowledgeable of, and consistently follow the procedures and processes for performing this task.	❒	❒	
5.4.2.17 Quality: A process and criteria exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	
5.4.2.18 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒
Not Applicable		❒	**Not Observed**	❒

Evidence Collected

Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement

- Build a strategy for learning about new technologies. It can include having staff members participate in
  - vendor presentations, conferences, or demonstrations
  - organizational discussions on new equipment purchasing plans (to understand what skills and knowledge will be needed to support changes in the operating environment)
  - professional development activities for staff to learn new skills (e.g., classes, conferences)

5.5 SECURITY ADMINISTRATION

5.5.1 Physical protective measures are in place to protect incident management IT systems, facilities, and personnel.

Priority I

Clarification

The intent of this capability is to ensure measures are implemented to protect incident management IT systems, facilities (e.g., rooms, buildings), information, and personnel who perform incident management functions. Since incident management personnel will be collecting, accessing, and storing sensitive information that relates to its organization, appropriate physical controls over the environment should be in place to protect these systems. In many cases, these protection strategies become the "example of best practice behaviors" for the rest of the organization and, as a result, incident management personnel exemplify a higher standard of practice. These practices usually address protection of not only the IT systems but also the physical space and the personnel working in that space. Access cards, for example, protect an entire area, including people and equipment. These measures should comply with relevant standards, guidelines, or organizational policies.

Team Guidance

The team should identify the relevant policies, standards, and regulations for securing the facilities and space within which incident management systems and personnel reside. Generally, the team should look for evidence that multiple levels of physical security exist and that access to the facility, spaces, information, and equipment is controlled, granted, verified, documented, and monitored. Physical protective measures may include but are not limited to lockable rooms or buildings, access controls, and alarms. All standards, regulations, and policies for physical security should be documented. Team members can observe how access is controlled when they themselves are given access. The team can check for the organization's adherence to relevant standards, guidelines or policies by conducting interviews with the organization's physical security or ISOs (and verifying if systems need to meet High or Medium requirements), or by reviewing any SSP or similar audit report for the organization's facilities.

References

Regulatory References:

FISMA Sec 3544 *Federal agency responsibilities* (b)(3) [OLRC 2003]

> "(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] to provide information security for the information and information systems that support the operations and assets of the agency […] that includes—
>
> (3.) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate"

FIPS 200 *Minimum Security Requirements for Federal Information and Information Systems* [NIST 2006]

> "Physical and Environmental Protection (PE): Organizations must: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized

individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities."

FIPS 199 *Standards for Security Categorization of Federal Information and Information Systems* [NIST 2004]

> "FIPS Publication 199 addresses the first task cited—to develop standards for categorizing information and information systems. Security categorization standards for information and information systems provide a common framework and understanding for expressing security that, for the Federal government, promotes: (i) effective management and oversight of information security programs, including the coordination of information security efforts throughout the civilian, national security, emergency preparedness, homeland security, and law enforcement communities; and (ii) consistent reporting to the Office of Management and Budget (OMB) and Congress on the adequacy and effectiveness of information security policies, procedures, and practices."

Guidance References:

NIST SP 800-53 Rev 4 *Security and Privacy Controls for Federal Information Systems and Organizations* [NIST 2013]

> FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION
> CLASS: OPERATIONAL

Organization Response

Examples of Evidence Sought

- ❑ Current lists of authorized individuals who have access to area(s) related to incident management activities, personnel, or facilities
- ❑ Up-to-date list of management POCs to notify when controls or regulations are broken
- ❑ Examples of any forms used for changes in protection measures
- ❑ Logs for unescorted and escorted personnel
- ❑ Access controls for visitors (escort requirements, badges, etc.) related to incident management activities, personnel or facilities
- ❑ Alarms (e.g., fire, flood, entry, other alarmed devices)
- ❑ Evidence of restricted hours
- ❑ Safes or other sensitive systems located in secured areas related to incident management
- ❑ Biometric devices
- ❑ TV cameras
- ❑ Swipe cards
- ❑ 24/7 guard
- ❑ Results of physical security audits or tests for compliance with relevant standards, guidelines, or policies
- ❑ Documented procedures for badging, escorting visitors, and background checks
- ❑ Copy of SSP or other audit report that assess compliance with 800-53 Rev 4 PE controls

Scoring Criteria	Yes	No	Evidence
Required			
5.5.1.01 Control: Physical security policies, protective measures, processes, and methods by which incident management personnel, information, IT systems, and the physical environment are protected are identified, documented, and kept up to date.	❒	❒	
5.5.1.02 Control: Personnel are trained appropriately on the processes for physical security, including how to identify and report insecurities.	❒	❒	
5.5.1.03 Activity: Physical protection measures are put in place and maintained.	❒	❒	
5.5.1.04 Activity: Personnel follow physical protection strategies and processes.	❒	❒	
5.5.1.05 Activity: Physical security controls comply with relevant standards, guidelines, or policies.	❒	❒	
Recommended Best Practices			
5.5.1.06 Control: An up to date, accurate, and complete list exists of the locations where all critical incident management information, equipment, and people are situated along with the protections required for each.	❒	❒	
5.5.1.07 Control: A protection training plan is documented for all personnel, and completion of that training is monitored.	❒	❒	
5.5.1.08 Activity: Personnel receive annual “refresher” training on protection measures.	❒	❒	
Institutional and Quality Improvement			
5.5.1.09 Control: Documented procedures exist for admitting and monitoring visitors to facilities.	❒	❒	
5.5.1.10 Control: Physical security procedures are documented and kept up-to-date, and describe the process and method by which the incident management IT systems and physical environment are protected.	❒	❒	
5.5.1.11 Quality: Personnel are aware of and understand protection measures and why they are needed.	❒	❒	

5.5.1.12 Quality: A process and criteria exist for evaluating the quality and effectiveness of protective measures.	❒	❒	
5.5.1.13 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒
Not Applicable		❒	**Not Observed**	❒

Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement

- Define controls for restricting access to critical resources with need-to-know requirements.
- Make the protective measures for non-required supporting mechanisms more robust (e.g., camera/monitoring service for visual access, swipe cards with anti-passback features).

5.5 SECURITY ADMINISTRATION

5.5.2 An operations security (OPSEC) program exists. Priority I

Clarification

This capability focuses on operational security: identifying and protecting information that might provide attackers with information about an organization's incident management plans or capabilities. The organization should have a formal OPSEC program for ensuring that all incident management personnel are sensitive to how information and data are created, handled, stored, retained, archived, and destroyed, and recognize the importance of OPSEC in protecting that data and information.

Team Guidance

The team should look for evidence of a formal OPSEC program, including policies and training records. The team also needs to verify (through interviews as well as actual training records) that incident handling personnel have been trained; are aware of and able to fulfill their roles and responsibilities; and know how to recognize and report OPSEC incidents. OPSEC information, including roles, responsibilities, and procedures, may be available for review via a website, visible postings such as wall posters, and reminders to personnel. The people interviewed by the team should demonstrate knowledge and understanding of OPSEC.

It should not matter who maintains this program: What is important is that one exists for the organization and it is followed by incident management personnel.

References

Regulatory References: None

[indirect]

FISMA Sec 3544 *Federal agency responsibilities* (b)(3) [OLRC 2003]

> "(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] to provide information security for the information and information systems that support the operations and assets of the agency […] that includes—
>
> (3.) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate"

Guidance References: None

[indirect]

NIST SP 800-53 Rev 4 *Security and Privacy Controls for Federal Information Systems and Organizations* [NIST 2013]

> "AT-2 SECURITY AWARENESS
>
> **Control:** The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors):
>
> (a.) As part of initial training for new users;
>
> (b.) When required by information system changes; and

(c.) [*Assignment: organization-defined frequency*] thereafter.

Supplemental Guidance: Organizations determine the appropriate content of security awareness training and security awareness techniques based on the specific organizational requirements and the information systems to which personnel have authorized access. […]"

AT-3 ROLE-BASED SECURITY TRAINING

Control: The organization provides role-based security training to personnel with assigned security roles and responsibilities:

(a.) Before authorizing access to the information system or performing assigned duties;

(b.) When required by information system changes; and

(c.) [*Assignment: organization-defined frequency*] thereafter.

Supplemental Guidance: Organizations determine the appropriate content of security training based on the assigned roles and responsibilities of individuals and the specific security requirements of organizations and the information systems to which personnel have authorized access. […] Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. […]"

NIST SP 800-61 Rev 2 *Computer Security Incident Handling Guide* [Cichonski 2012]

"Sec 2.6 Recommendations
[p 2-16]

Establish policies and procedures regarding incident-related information sharing."

Organization Response

Examples of Evidence Sought

- ❑ Samples of OPSEC awareness materials, templates for reporting failures/other insecurities, and so forth
- ❑ Videos and other awareness aids such as mousepads, magnets, or buttons
- ❑ Posted or distributed OPSEC flyers or other awareness aids
- ❑ Mechanisms for reporting OPSEC failures (e.g., templates, forms, processes, procedures)
- ❑ Mechanisms for providing information to personnel (e.g., websites, email, posters, meetings, presentations)

Scoring Criteria	Yes	No	Evidence
Required			
5.5.2.01 Prerequisite: A formal OPSEC program exists.	❒	❒	
5.5.2.02 Prerequisite: Critical information that is to be protected has been identified.	❒	❒	
5.5.2.03 Control: Documented policies exist specifying that potentially exploitable information must be protected.	❒	❒	

5.5.2.04 Control: Information about the OPSEC program including roles, responsibilities, and POCs exists and is available to all personnel.	❒	❒	
5.5.2.05 Activity: Personnel receive formal or informal OPSEC training, briefings, and information.	❒	❒	
5.5.2.06 Activity: Personnel receive refresher training (monthly, quarterly, semi-annually, etc.).	❒	❒	
5.5.2.07 Quality: OPSEC information is up to date, accurate, and relevant.	❒	❒	
5.5.2.08 Activity: The OPSEC program tracks the completion of OPSEC training.	❒	❒	
Recommended Best Practices			
5.5.2.09 Activity: Personnel receive role-based OPSEC training.	❒	❒	
Institutional and Quality Improvement			
5.5.2.10 Control: Documented procedures exist describing how to protect potentially exploitable information.	❒	❒	
5.5.2.11 Quality: A process and criteria exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	
5.5.2.12 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒	
Not Applicable		❒	**Not Observed**	❒	
Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement
• Schedule speakers to present case studies or other scenarios to train personnel on OPSEC. • Use other methods (e.g., contests) to educate personnel about OPSEC. • Conduct periodic walk-throughs of the physical workspaces to review and identify potential insecurities.

5.6 IM INFORMATION SYSTEMS

5.6.1 An inventory exists of mission-critical incident management systems, data, and information.

Priority I

Clarification

This capability ensures that mission-critical systems and data for incident management have been identified and an up-to-date inventory is maintained by incident management personnel so a better prioritized maintenance, response, and remediation can be performed. This capability is an essential part of maintaining a defense-in-depth capability.

This capability focuses on understanding the systems, data, or information critical to the management of incidents. Current information should be available about what is on IM networks and systems to best assess protection requirements and ensure a timely and appropriate response. Having up-to-date information also helps ensure legal compliance with regulations or laws (e.g., to make sure information is released or accessed in an authorized fashion). When an event, incident, or vulnerability occurs that effects IM systems and data, impacts can be assessed in light of the data's or system's criticality.

Team Guidance

The team should determine if an inventory exists and if it is up to date. There should be a list of critical assets and a process for keeping the list current and accurate. If possible, up-to-date configuration information should be available for all IM networks and systems. Configuration information can include

- a list of IP address ranges and responsible administrative personnel or ISOs
- the latest organizational network diagrams for IM systems
- an up-to-date inventory of information systems, network components, application software, OSs, and network services used by the IM function

This inventory may also be part of a larger organizational inventory. If so, incident management systems, data, and inventory need to be clearly identified as such.

References

Regulatory References: None

[indirect]

FIPS 199 *Standards for Security Categorization of Federal Information and Information Systems* [NIST 2004]

> "FIPS Publication 199 addresses the first task cited—to develop standards for categorizing information and information systems. Security categorization standards for information and information systems provide a common framework and understanding for expressing security that, for the Federal government, promotes: (i) effective management and oversight of information security programs, including the coordination of information security efforts throughout the civilian, national security, emergency preparedness, homeland security, and law enforcement communities; and (ii) consistent reporting to the Office of Management and

Budget (OMB) and Congress on the adequacy and effectiveness of information security policies, procedures, and practices."

Guidance References:

NIST 800-61 Rev 2 *Computer Security Incident Handling Guide* [Cichonski 2012]

"Sec 3.2.6 Incident Prioritization
Prioritizing the handling of the incident is perhaps the most critical decision point in the incident handling process. Incidents should not be handled on a first-come, first-served basis as a result of resource limitations. Instead, handling should be prioritized based on the relevant factors, such as the following:

- Functional Impact of the Incident…
- Information Impact of the Incident. …
- Recoverability from the Incident."

[indirect]

NIST SP 800-59 *Guideline for Identifying an Information System as a National Security System* [Barker 2003]

"Accordingly, the purpose of these guidelines is not to establish requirements for national security systems, but rather to assist agencies in determining which, if any, of their systems are national security systems as defined by FISMA and are to be governed by applicable requirements for such systems, issued in accordance with law and as directed by the President."

Agency Response

Examples of Evidence Sought

- ❑ Up-to-date list or database of critical IM systems, data, and information
- ❑ Up-to-date list of POCs responsible for and/or knowledgeable of critical IM systems, data, and information

Scoring Criteria	Yes	No	Evidence
Required			
5.6.1.01 Control: A documented process exists establishing an inventory of critical IM systems, data, and information.	❒	❒	
5.6.1.02 Control: A process or guidance exists for contacting the personnel responsible for critical IM systems, data, and information.	❒	❒	
5.6.1.03 Control: Incident management personnel are trained appropriately on the processes and technologies employed to obtain, store, and use this information.	❒	❒	

5.6.1.04 Activity: An inventory of mission-critical IM systems, data, information, and associated POCs is established and maintained.	❒	❒	
5.6.1.05 Activity: The list of critical IM systems, services, data, and information is archived in a secure and protected manner.	❒	❒	
Recommended Best Practices			
5.6.1.06 Prerequisite: Criteria exist that define which systems, data, and information are IM-mission critical.	❒	❒	
5.6.1.07 Activity: A database or other mechanism is used to track mission-critical IM systems, data, information, and corresponding POCs.	❒	❒	
Institutional and Quality Improvement			
5.6.1.08 Control: Documented procedures exist that describe the process and method by which the inventory of mission-critical IM systems and data is obtained, stored, and used.	❒	❒	
5.6.1.09 Quality: The inventory is sufficiently detailed to enable analysts to determine whether an event or incident affects mission-critical IM systems, data, or information.	❒	❒	
5.6.1.10 Quality: Personnel are aware of, knowledgeable of, and consistently follow the procedures, processes, methodologies, and technologies for collecting and using this information.	❒	❒	
5.6.1.11 Quality: A process and criteria exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	
5.6.1.12 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒
Not Applicable		❒	**Not Observed**	❒

Evidence Collected					
Document Review		Interviews		Direct Observation	
Notes					
Suggestions for Improvement					
None					

5.6 IM INFORMATION SYSTEMS

5.6.2 Defense-in-depth strategies and methodologies exist for hardening the incident management computer networks and systems.

Priority I

Clarification

The intent of this capability is to ensure the incident management function has multiple layers of security protection strategies for hardening its systems, network, and information assets. It is even more critical that the systems owned and operated by incident management personnel use the same or better security as required for the broader organization's systems. The defense-in-depth strategy should ensure there are no single points of failure in the protection of the systems and networks that support incident management activities. The resulting in-depth defenses limit the opportunities for attacks and threats to be successful in breaching security. Physical security may need to follow organizational or other standards such as NIST SP 800-53. Defense in depth means implementing multiple tiers of security for incident management networks and working environments, for example

- multi-factor authentication is used.
- physical security controls are set up for facilities access and building security.
- host- and network-based IDSs or IPSs are installed on incident management mission-critical systems.
- firewalls are used to segment the IM networks.
- a DMZ is set up for public web, DNS, and email servers.
- AV software is installed on all workstations and critical servers.
- monitoring tools for content security are installed.
- ACLs are used to protect IM data and the applications and systems they reside on.
- unnecessary network protocols, ports, and services are blocked.
- email is scanned, filtered, and blocked per NIST 800-45.
- systems and components are configured according to the principle of "least functionality."

Team Guidance

The team should look for evidence of a defined, defense-in-depth strategy and plan that have been implemented to protect the organization's incident management assets. The strategy should clearly identify the different means and levels of security for the systems and networks. The team should look for single points of failure, gaps, or single layers of coverage in the strategy and implemented plans. The team should also verify that the security layers are updated and maintained routinely, and verify that incident management personnel have been trained on the defense-in-depth strategy, methods, procedures, and tools. Any organizational requirements or guidance should be followed.

References

Regulatory References: None

[indirect]

FISMA Sec 3544 *Federal agency responsibilities* (b)(3) [OLRC 2003]

> "(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] to provide information security for the information and information systems that support the operations and assets of the agency […] that includes—
>
> (3) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate"

FIPS 200 *Minimum Security Requirements for Federal Information and Information Systems* [NIST 2006]

> "The minimum security requirements cover seventeen security-related areas with regard to protecting the confidentiality, integrity, and availability of Federal information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: (i) access control; (ii) awareness and training; (iii) audit and accountability; (iv) certification, accreditation, and security assessments; (v) configuration management; (vi) contingency planning; (vii) identification and authentication; (viii) incident response; (ix) maintenance; (x) media protection; (xi) physical and environmental protection; (xii) planning; (xiii) personnel security; (xiv) risk assessment; (xv) systems and services acquisition; (xvi) system and communications protection; and (xvii) system and information integrity."

Guidance References:

NIST SP 800-53 Rev.4 *Security and Privacy Controls for Federal Information Systems and Organizations* [NIST 2013]

> "The purpose of this publication is to provide guidelines for selecting and specifying security controls for organizations and information systems supporting the executive agencies of the Federal government to meet the requirements of FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*. The guidelines apply to all components of an information system that process, store, or transmit Federal information."
>
> [indirect]

NIST SP 800-14 *Generally Accepted Principles and Practices for Securing Information Technology Systems* [Swanson 1996]

> "As more organizations share information electronically, a common understanding of what is needed and expected in securing information technology (IT) resources is required. This document provides a baseline that organizations can use to establish and review their IT security programs."

NIST SP 800-18 Rev 1 *Guide for Developing Security Plans for Federal Information Systems* [Swanson 2006]

> "Today's rapidly changing technical environment requires Federal agencies to adopt a minimum set of security controls to protect their information and information systems. Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*, specifies the minimum security requirements for Federal information and information systems in seventeen security-related areas. Federal agencies must meet the minimum security requirements defined in FIPS 200 through the use of the security controls in NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*. NIST SP 800-53 contains the management, operational, and technical safeguards or countermeasures prescribed for an information system. The controls selected or planned must be documented in a system security plan. This document provides guidance for Federal agencies for developing system security plans for Federal information systems."

Organization Response

Examples of Evidence Sought
❑ Rule sets for an IDS/IPS ❑ Scheduled or automatic updates enabled for monitoring tools ❑ Schedule for AV signature updates ❑ Audit records for security audits ❑ Annual security review of systems to identify and mitigate security risks ❑ SSP for IM systems ❑ Observation of physical controls in place to protect IM facilities, systems, and people ❑ Training materials on protecting IM data and equipment ❑ Training records showing IM personnel have taken training and refreshers on defense in depth ❑ Procedures and guidance describing defense in depth strategies and how they are to be implemented and followed in the IM function and for related equipment ❑ Audit records from SSP or other security assessment ❑ Records showing compliance with FIPS 199 ❑ System design documentation, implementation guides, procedures, and user guides that describe defense in depth built into or applied to IM systems, applications, and networks ❑ Observation of defense-in-depth strategies (mentioned in clarification) in practice

Scoring Criteria	Yes	No	Evidence
Required			
5.6.2.01 Control: There is a defense-in-depth strategy and plan.	❒	❒	
5.6.2.02 Control: POCs are identified, and roles and responsibilities are assigned for protecting and defending incident management systems.	❒	❒	
5.6.2.03 Control: Personnel are appropriately trained on the relevant defense-in-depth methods and technologies.	❒	❒	
5.6.2.04 Control: Personnel understand how to report insecurities or failures in any defense mechanisms.	❒	❒	
5.6.2.05 Control: Only authorized users have access to incident-management-related systems and networks.	❒	❒	
5.6.2.06 Activity: Defense-in-depth methods and technologies are identified and implemented for the IM function.	❒	❒	

5.6.2.07 Activity: Designated personnel review and maintain defense-in-depth components and documents.	❒	❒	
5.6.2 8 Activity: The defense-in-depth methods and technologies are assessed at least annually against the plan for effectiveness and completeness, and improvements are made as needed.	❒	❒	
Recommended Best Practices			
5.6.2.09 Control: A documented, known strategy exists for implementing and maintaining appropriate defense in depth.	❒	❒	
5.6.2.10 Activity: Defense-in-depth, role-based training is implemented for all personnel who maintain or administer the organization's IT infrastructure, with annual refreshers.	❒	❒	
Institutional and Quality Improvement			
5.6.2.11 Control: Documented procedures exist for implementing defense in depth.	❒	❒	
5.6.2.12 Control: Documented procedures exist that define the methods and mechanisms for installing, replacing, and updating/upgrading systems and networks to improve defense in depth.	❒	❒	
5.6.2.13 Quality: Personnel are aware of, knowledgeable of, and consistently follow the procedures.	❒	❒	
5.6.2.14 Quality: A process and criteria exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	
5.6.2.15 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒
Not Applicable		❒	**Not Observed**	❒

Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement

- Conduct QA tests or checks of security products and tools to ensure they are current and up to date.
- Conduct mock exercises or penetration testing to test defense-in-depth methods and determine if they are working.
- Implement products from different vendors to provide more robust coverage and avoid single points of failure; for example, use AV products from competing vendors on PCs and servers, or multiple AV products on the same devices.
- If any tools are developed in-house, implement code reviews and testing for insecurities (security "walk-throughs").

5.6 IM INFORMATION SYSTEMS

5.6.3 Processes and technologies exist to support the confidentiality, integrity, and availability of incident management data and information.

Priority I

Clarification

This capability focuses on the ability of the organization to protect the confidentiality, integrity, and availability (CIA) of its data and information, not only for incident management but also for any constituent information that incident management personnel receive, handle, transmit, store, or archive. Without effective measures to protect information and ensure it hasn't been modified, deleted, or inappropriately accessed, the organization might be at risk. Sensitive information collected as part of incident management activities (e.g., vulnerable systems, personal information) needs to be protected to ensure it has not been "tainted," viewed, copied, modified, or deleted. Having robust protection strategies in place to protect these assets will maintain confidential information, ensure it is available to those who are authorized to see and use it, and ensure it has not been modified inappropriately.

Team Guidance

The team should verify that the IM function (or the larger organization) has well-defined policies and procedures in place for protective and defensive strategies, and that personnel are knowledgeable about, consistently use, and support the repeatable processes for handling information commensurate with the various security levels.

References

Regulatory References:

FISMA Sec 3544 *Federal agency responsibilities* (b)(3) [OLRC 2003]

> "(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] to provide information security for the information and information systems that support the operations and assets of the agency […] that includes—
>
> (3) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate"

Guidance References: None

[indirect]

NIST SP 800-14 *Generally Accepted Principles and Practices for Securing Information Technology Systems* [Swanson 1996]

> "As more organizations share information electronically, a common understanding of what is needed and expected in securing information technology (IT) resources is required. This document provides a baseline that organizations can use to establish and review their IT security programs."

NIST SP 800-18 Rev 1 *Guide for Developing Security Plans for Federal Information Systems* [Swanson 2006]

> "Today's rapidly changing technical environment requires Federal agencies to adopt a minimum set of security controls to protect their information and information systems. Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*, specifies the minimum security requirements for Federal information and information systems in seventeen security-related areas. Federal agencies must meet the minimum security requirements defined in FIPS 200 through the use of the security controls in NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*. NIST SP 800-53 contains the management, operational, and technical safeguards or countermeasures prescribed for an information system. The controls selected or planned must be documented in a system security plan. This document provides guidance for Federal agencies for developing system security plans for Federal information systems."

NIST SP 800-53 Rev 4 *Security and Privacy Controls for Federal Information Systems and Organizations* [NIST 2013]

> "The purpose of this publication is to provide guidelines for selecting and specifying security controls for organizations and information systems supporting the executive agencies of the Federal government to meet the requirements of FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*. The guidelines apply to all components of an information system that process, store, or transmit Federal information."

Organization Response

Examples of Evidence Sought

- ❑ Results from monitoring audit files (to ensure protection/detection tools are functioning as expected)
- ❑ Demonstrations or observations of physical and electronic protective measures (safes, ACLs, shredders, evidence of use of encryption, etc.)
- ❑ Copies of backups (files, equipment, application software)
- ❑ Demonstrations of appropriate technology (e.g., PKI, PGP, GnuPG, or secure virtual private network [VPN]; secure email/voice/FAX) to support CIA during transmission, processing, and storage (e.g., AVS on workstations and servers)
- ❑ Demonstrations or observations of secure data storage to support the CIA of data and information, such as fireproof and waterproof containers for backup tapes, remote storage for backups, secure access-controlled room with fire and environmental safeguards, and appropriate labeling of backups

Scoring Criteria	Yes	No	Evidence
Required			
5.6.3.01 Control: Requirements are defined for the CIA of data and information.	❒	❒	

5.6.3.02 Control: Personnel are appropriately trained on the policies and relevant technology.	❒	❒	
5.6.3.03 Activity: Data and information are protected as required during collection, transmission, storage, review, and manipulation.	❒	❒	
5.6.3.04 Activity: Appropriate technology is used to secure the transmission of sensitive information between constituents, IM personnel, and any external entities (sites, regulatory bodies, LE, other incident management groups, etc.).	❒	❒	
Recommended Best Practices			
5.6.3.05 Control: All personnel are trained on how to respond to any breach of protected data.	❒	❒	
Institutional and Quality Improvement			
5.6.3.06 Control: Documented procedures exist for protecting the CIA of data and information.	❒	❒	
5.6.3.07 Quality: Personnel are aware of, knowledgeable of, and consistently follow the procedures for this activity.	❒	❒	
5.6.3.08 Quality: A process and criteria exist (including timeliness and accuracy) for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	
5.6.3.09 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒	
Not Applicable		❒	**Not Observed**	❒	
Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement
• Incorporate encryption solutions for off-site storage of backup and archived data. • Arrange risk assessments, conduct self-assessments, or use independent evaluations to validate processes and procedures for how data and information are handled, processed, transmitted, accessed, stored, and destroyed.

5.6 IM INFORMATION SYSTEMS

5.6.4 Network security monitoring is performed on all incident-management-related networks and systems.

Priority I

Clarification

The intent of this capability is to ensure incident management personnel are watching their own networks. A documented and implemented plan should exist for monitoring incident management systems to protect information assets. This monitoring plan should include methods for detecting events, incidents, anomalous activity, intrusion attempts, and other potential threats. It also requires knowing what the critical incident management systems, components, and assets are to appropriately focus the monitoring activity.

Information collected by incident management personnel and stored on incident management systems and applications such as incident tracking systems, data analytics engines, or constituency contact lists can contain sensitive information. This information often includes details about vulnerabilities and weaknesses in the organizational infrastructure. It is critical that such information be protected with the same rigor applied to other key organizational data and assets. The incident management function should strive to operate as a model to other organizational components in the protection and defense of the organization's critical systems and data.

Technologies involved in network monitoring and analysis can include IDSs, IPSs, ADSs, AVSs, netflow analysis tools, network forensic analysis tools, and other similar tools.

Team Guidance

Documented policies should exist that require and direct the monitoring of incident management personnel's own systems and networks. Documentation of what is considered critical should drive the policies or be incorporated into a plan. The team should look for

- installed and functioning tools
- tool reports
- event/alert analyses
- logs
- other evidence that the tools exist and are installed and used properly
- evidence that any alerts or events are resolved

If the organizational components being interviewed state that all incident management systems are monitored as part of the normal infrastructure monitoring, that is an acceptable answer. However, they should still show that the regular monitoring plan incorporates those systems.

This function might be outsourced or handled by another part of the organization. In that case, this capability should be applied to that group and its activities.

The key here is that specific actions are taken to monitor systems and networks used in the performance of incident management activities such as monitoring, detection, analysis, tracking, and response. The activity does not have to be performed by incident management personnel. Another part of the organization can do it and then notify the incident management function about any concerns, attacks, or other problems and issues. Note that to be practical, the organization

may not detect 100% of intrusions, although they certainly want to catch almost all, or at least the critical ones. It is easy to claim to handle all of the intrusions detected when only a small percentage are actually being caught.

References

Regulatory References: None

Guidance References:

NIST SP 800-53 Rev 4 *Security and Privacy Controls for Federal Information Systems and Organizations* [NIST 2013]

> "CA-7 CONTINUOUS MONITORING
>
> Control: The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:
>
> (a.) Establishment of [*Assignment: organization-defined metrics*] to be monitored;
> (b.) Establishment of [*Assignment: organization-defined freq*uencies] for monitoring and [*Assignment: organization-defined freq*uencies] for assessments supporting such monitoring;
> (c.) Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;
> (d.) Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy;
> (e.) Correlation and analysis of security-related information generated by assessments and monitoring;
> (f.) Response actions to address results of the analysis of security-related information; and
> (g.) Reporting the security status of organization and the information system to [*Assignment: organization-defined personnel or roles*] [*Assignment: organization-defined frequency*].
>
> SI-4 INFORMATION SYSTEM MONITORING
>
> Control: The organization:
>
> (a.) Monitors the information system to detect:
> 1. Attacks and indicators of potential attacks in accordance with [*Assignment: organization-defined monitoring objectives*]; and
> 2. Unauthorized local, network, and remote connections;
> (b.) Identifies unauthorized use of the information system through [*Assignment: organization-defined techniques and methods*];
> (c.) Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization;
> (d.) Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
> (e.) Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; and
> (f.) Obtains legal opinion with regard to information system monitoring activities in accordance with applicable Federal laws, Executive Orders, directives, policies, or regulations."

NIST Interagency Report 7756 Draft *CAESARS Framework Extension: An Enterprise Continuous Monitoring Technical Reference Architecture* [Mell 2012]

"The end goal of CAESARS FE is to enable enterprise CM by presenting a technical reference architecture that allows organizations to aggregate collected data from across a diverse set of security tools, analyze that data, perform scoring, enable user queries, and provide overall situational awareness."

DHS Continuous Asset Evaluation, Situational Awareness, and Risk Scoring Reference Architecture Report (CAESARS) [DHS 2010]

"The objective of this document is to describe a reference architecture that is an abstraction of a security posture monitoring and risk scoring system, informed by the sources noted above, and that can be applied to other agencies seeking to apply risk scoring principles to their information security program."

Organization Response

Examples of Evidence Sought

- ❑ Samples of logs, alerts, and reports generated by network security monitoring tools
- ❑ Network diagrams showing placement of monitoring tools on organizational networks
- ❑ IDS, IPS, ADS, or AVS configuration files that specify what anomalous events trigger an alarm
- ❑ Documentation of actions for responding to alerts and reports generated by network security monitoring tools
- ❑ Observations of actual monitoring activities including devices, software, and outputs
- ❑ Recent audit logs from network and system monitoring tools
- ❑ Reports from monitoring activities
- ❑ Results of testing the monitoring of critical network segments
- ❑ Mechanism for controlling physical access to systems (e.g., by foreign nationals or visitors)

Scoring Criteria	Yes	No	Evidence
Required			
5.6.4.01 Control: Criteria exist for characterizing anomalous events, including suspicious ports, protocols, and services (both network based and host based).	❒	❒	
5.6.4.02 Control: Documented guidance exists requiring the continuous monitoring of incident management networks and systems.	❒	❒	
5.6.4.03 Control: Personnel are trained in the processes and supporting technologies used to monitor the incident management systems and networks.	❒	❒	

5.6.4.04 Control: Monitoring of incident management systems and networks follows, at a minimum, the same level of monitoring done on other organizational systems and networks.	❒	❒	
5.6.4.05 Control: Only authorized users have the access needed to monitor incident-management-related systems and networks.	❒	❒	
5.6.4.06 Control: A plan exists for responding to incidents against the incident management systems.	❒	❒	
5.6.4.07 Activity: Security monitoring is conducted on all incident-management-related networks and systems.	❒	❒	
5.6.4.08 Activity: Anomalous network events are characterized in support of network monitoring and intrusion detection.	❒	❒	
5.6.4.09 Activity: The output from monitoring tools is reviewed and analyzed to detect an event or potential incident.	❒	❒	
5.6.4.10 Activity: Reports of alerts and notifications are forwarded to other organizations as specified by organizational policy or guidance.	❒	❒	
5.6.4.11 Activity: Real-time or near real-time analysis is performed on data collected from the incident management networks and systems.	❒	❒	
5.6.4.12 Activity: Any intrusions or threats against incident management systems are mitigated or resolved.	❒	❒	
5.6.4.13 Quality: Backup and recovery capabilities exist in the form of spare equipment for any network or host monitoring tools.	❒	❒	
Recommended Best Practices			
5.6.4.14 Control: Network diagrams exist showing placement of monitoring tools such as sensors on incident management networks.	❒	❒	
5.6.4.15 Activity: Analysis/support personnel are available 24/7.	❒	❒	
Institutional and Quality Improvement			
5.6.4.16 Control: Documented procedures exist that define how incident management networks should be monitored and analyzed.	❒	❒	

5.6.4.17 Quality: Personnel are aware of, knowledgeable of, and consistently follow the procedures, processes, and methodologies for performing this task.	❒	❒	
5.6.4.18 Quality: A process and criteria exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	
5.6.4.19 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒
Not Applicable		❒	**Not Observed**	❒

Evidence Collected

Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement

- Use automated tools.
- Ensure automated alerts are enabled.
- Implement multiple types of network monitoring systems.
- Ensure results are analyzed in near-real-time.
- Ensure network diagrams of monitoring system placement are available and up to date.

5.6 IM INFORMATION SYSTEMS

5.6.5 Security risk assessments (RAs) are performed on the incident management function.

Priority I

Clarification

This capability focuses on the ability of the organization to perform security RAs on the incident management function, including its systems, networks, and practices. This includes having a capability for

- public and private monitoring of information sources and organizations (such as vendor and security sites, and other similar organizations) for information about security RAs
- keeping up to date on current weaknesses, vulnerability threats, attacks, and remediation strategies (through research, training, mentoring, and attending courses and other forms of professional development)
- coordinating with other internal and external parties to schedule, conduct, and review the results of such assessments
- properly reporting to approved individuals and/or upper management
- implementing fixes and mitigation for risks identified during analysis (this includes categorizing, prioritizing, and assessing the impact to incident management systems and practices)

Organizational collaboration and coordination will require internally defined processes, roles, and responsibilities.

The scope of this capability is broader than Certification and Accreditation (C&A) activities, which focus on addressing security risks to information systems. C&A is a systematic procedure for evaluating, describing, testing, and authorizing an information system prior to or after it is in operation to ensure that it operates within an acceptable level of risk. C&A activities are limited to an organization's information systems; they do not assess organizational security risks. As a result, C&A, by itself, does not address the full extent of this capability. Note that this is different from capability 2.1.1 which is concerned with security RAs on the entire organization.

Team Guidance

The team should determine that the organization can consistently, accurately, and reliably conduct security RAs on its incident management systems and networks, and implement strategies to remove or mitigate risk to an acceptable level. Note that the prerequisite states that incident management personnel have approval (from management or other authorized individuals) to conduct such assessments. However, if they do not perform this activity, some other part of the organization may do it on their behalf. Regardless of who performs the assessments, current documentation and information on the systems' criticality and assets must be identified. Without this information, risk or threat can only be evaluated in an abstract, theoretical sense. Look for evidence that security RAs were conducted (e.g., security RA methods or tools, reports, lists of identified risks, recommendations) and the results were used to make improvements (e.g., implemented mitigation plans, actions taken in reference to specific risks). The team may need to interview someone who performs the RAs if they are not done by incident management personnel.

References

Regulatory References:

FISMA Sec 3544 *Federal agency responsibilities* (b)(1) [OLRC 2003]

> "(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] to provide information security for the information and information systems that support the operations and assets of the agency […] that includes—
>
> (1) periodic assessments of the risk […]"

FIPS 199 *Standards for Security Categorization of Federal Information and Information Systems* [NIST 2004]

> "FIPS Publication 199 addresses the first task cited—to develop standards for categorizing information and information systems."

Guidance References: None

[indirect]

NIST 800-39 *Managing Information Security Risk: Organization, Mission, and Information System View* [NIST 2011]

> "NIST SP 800-39 is the flagship document in the series of information security standards and guidelines developed by NIST in response to FISMA.
>
> 2.1 COMPONENTS OF RISK MANAGEMENT
>
> The second component of risk management addresses how organizations *assess* risk within the context of the organizational risk frame."

NIST 800-37 Rev 1 *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Lifecycle Approach* [NIST 2010]

> "The purpose of this publication is to provide guidelines for applying the Risk Management Framework to Federal information systems […]."

NIST SP 800-60 Rev. 1 *Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories* [Stine 2008]

> "NIST SP 800-60 addresses the FISMA direction to develop guidelines recommending the types of information and information systems to be included in each category of potential security impact."

NIST SP 800-30 *Guide for Conducting Risk Assessments* [JTFTI 2012]

> "The purpose of Special Publication 800-30 is to provide guidance for conducting risk assessments of Federal information systems and organizations."

NIST SP 800-53 Rev 4 *Security and Privacy Controls for Federal Information Systems and Organizations* [NIST 2013]

> "RA-3 Risk Assessment
>
> **Control:** The organization:
>
> (a.) Conducts an assessment of risk […];
> (b.) Documents risk assessment results […];
> (c.) Reviews risk assessment results [*Assignment: organization-defined frequency*];
> (d.) Disseminates risk assessment results to [*Assignment: organization-defined personnel or roles*]; and
> (e.) Updates the risk assessment […]"

DHS Continuous Asset Evaluation, Situational Awareness, and Risk Scoring Reference Architecture Report (CAESARS) [DHS 2010]

> "The objective of this document is to describe a reference architecture that is an abstraction of a security posture monitoring and risk scoring system, informed by the sources noted above, and that can be applied to other agencies seeking to apply risk scoring principles to their information security program."

ISO/IEC 31000, *Risk management—Principles and guidelines*

ISO/IEC 31010, *Risk management—Risk assessment techniques*

ISO/IEC 27001, *Information technology—Security techniques—Information security management systems—Requirements*

ISO/IEC 27005, *Information technology—Security techniques—Information security risk management systems*

Organization Response

Examples of Evidence Sought

- ❑ Copies of records, analysis results, or results of security RAs
- ❑ List of security RA types and providers with POC lists
- ❑ Mechanism for tracking and reporting risks and corrective actions
- ❑ Approved security RA methods and tools used in accordance with organizational requirements
- ❑ Documentation of implemented risk mitigation plans or actions taken to handle risks

Scoring Criteria	Yes	No	Evidence
Required			
5.6.5.01 Prerequisite: Management (or other authorized body) has given approval for conducting security RAs on the incident management function and processes.	❒	❒	
5.6.5.02 Control: Documented policies or guidance exist specifying that security RAs are conducted on the IM function and the results are analyzed.	❒	❒	
5.6.5.03 Control: Personnel are appropriately trained on the process and supporting technologies used to conduct security RAs and corresponding analysis.	❒	❒	
5.6.5.04 Activity: Security RAs are conducted on the incident management function, including its networks, systems, and practices.	❒	❒	

5.6.5.05 Activity: The Security RAs are used to determine potential impacts and make improvements to incident management infrastructure to prevent computer security incidents.	❒	❒	
5.6.5.06 Activity: The security RA results are provided to the appropriate individuals.	❒	❒	
5.6.5.07 Activity: The security RA results are archived in a secure and protected manner.	❒	❒	
5.6.5.08 Activity: The security RA results are communicated in a secure and protected manner in accordance with the sensitivity of the information.	❒	❒	
Recommended Best Practices			
5.6.5.10 Activity: Lessons learned from security RAs are incorporated into security RA processes, training, and testing.	❒	❒	
5.6.5.11 Activity: A list of organization-approved security RA methodologies (e.g., NIST guidance, COBIT, OCTAVE) is collected, maintained, and updated.	❒	❒	
5.6.5.12 Quality: A designated schedule (per organizational policy or guidance) is followed for performing security RAs (e.g., on a periodic/scheduled basis, when new systems are acquired, when an organizational change impacts incident management activities or systems).	❒	❒	
Institutional and Quality Improvement			
5.6.5.13 Control: Documented procedures exist describing the process and method used to conduct security RAs and analyze the results.	❒	❒	
5.6.5.14 Quality: Personnel are aware of, knowledgeable of, and consistently follow or use the procedures, processes, methodologies, and technologies for performing this task.	❒	❒	
5.6.5.15 Quality: A process and criteria (including completeness, frequency, adequacy, scope, and level of detail for security RAs) exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	

5.6.5.16 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.			❒	❒	
Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒	
Not Applicable		❒	**Not Observed**	❒	
Evidence Collected					
Document Review		Interviews		Direct Observation	
Notes					
Suggestions for Improvement					
• Perform certification and accreditation of incident management systems and networks as a means of reducing risk, in addition to performing security RAs.					

5.6 IM INFORMATION SYSTEMS

5.6.6 Vulnerability assessments are performed on incident management systems and networks.

Priority I

Clarification

This function focuses on whether the organization performs vulnerability assessments on incident management systems and networks to identify potential threats and problems. The goal is to ensure that vulnerabilities are identified and remediated faster than they can be exploited. A central part of vulnerability assessment is continually performing vulnerability scanning (VS). Once vulnerabilities have been identified, remediation activities can be prioritized.

Vulnerability assessments may be done by incident management personnel, another group of individuals within the organization, or an outside party qualified to conduct vulnerability assessments. In either case, management authorization must be obtained (preferably in written form) that describes the conditions and schedule under which such activities are performed. Vulnerability scanning tools should be run on a routine basis, as well as when warranted. Such scanning can provide warnings about weaknesses that may have an impact on the incident management infrastructure. Results from this vulnerability scanning can be used as a rationale for updates or changes in system and network configurations, or as justification for new components, system upgrades, or additional software and hardware. Incident management personnel should be familiar and up to date on their knowledge of vulnerability sources such as CVE, NVD, or vendor alerts. The same applies to the vulnerability scanning tools.

Policies and procedures should identify the guidelines and rules for scheduling, conducting, analyzing, and taking action on any information identified through such scanning activity.

Note that patch management is generally a part of vulnerability management. Patch management for IM systems is covered in capability 5.6.7.

Team Guidance

The team should determine if the organization conducts vulnerability assessments of incident management systems on a routine schedule. That schedule should be dictated by policy and involve scanning that is done both periodically (e.g., on a daily, weekly, or monthly basis) and as needed (whenever a potential threat warrants). In particular, incident management personnel should have identified the systems where critical assets reside and ensure they are scanned. The team should also look for evidence that scanning tools are used and personnel are trained how to use them properly. The team should also look for evidence that remediation is performed based on the results of the vulnerability assessments.

This function might be outsourced or handled by another part of the organization. In that case, this capability should be applied to that group and its activities.

References

Regulatory References:

FISMA Sec 3544 *Federal agency responsibilities* (b)(5) [OLRC 2003]

> "(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] to provide information security for the

information and information systems that support the operations and assets of the agency […] that includes— […]

(5) periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually, of which such testing—

(A) shall include testing of management, operational, and technical controls of every information system identified in the inventory required under Section 3505(c); and

(B) may include testing relied on in an evaluation under Section 3545"

Guidance References:

NIST SP 800-53 Rev 4 *Security and Privacy Controls for Federal Information Systems and Organizations* [NIST 2013]

"RA-5 Vulnerability Scanning
The organization:

(a.) Scans for vulnerabilities in the information system and hosted applications […];

(b.) Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process […]

(c.) Analyzes vulnerability scan reports and results from security control assessments;"

NIST SP 800-61 Rev 2 *Computer Security Incident Handling Guide* [Cichonski 2012]

NIST SP 800-115 *Technical Guide to Information Security Testing and Assessment* [Scarfone 2008]

"Sec 4.3 Vulnerability Scanning

Like network port and service identification, vulnerability scanning identifies hosts and host attributes (e.g., operating systems, applications, open ports), but it also attempts to identify vulnerabilities rather than relying on human interpretation of the scanning results. […]"

NIST SP 800-45 ver. 2 *Guidelines on Electronic Mail Security* [Tracy 2007]

"9.4.1 Vulnerability Scanning

Vulnerability scanners are automated tools that are used to identify vulnerabilities and misconfiguration of hosts. Many vulnerability scanners also provide information about mitigating discovered vulnerabilities. […]"

Organization Response

Examples of Evidence Sought

- ❑ Vulnerability scan reports
- ❑ POC list of authorized individuals who perform the vulnerability assessments
- ❑ Demonstration or observation of approved vulnerability scanning tools
- ❑ Records or indications of training on the tools
- ❑ Observation or demonstration of mechanisms for tracking and monitoring vulnerability assessment activities and archiving the results

- ❑ Records of improvements or corrections made based on the results of vulnerability assessments
- ❑ Walk-through of remediation process with examples

Scoring Criteria	Yes	No	Evidence
Required			
5.6.6.01 Prerequisite: Authorizations to perform vulnerability assessments have been provided (by procedures, documented roles and responsibilities, MOUs, email, policies, etc.).	❒	❒	
5.6.6.02 Control: Documented policies exist describing the requirements for vulnerability assessments.	❒	❒	
5.6.6.03 Control: Personnel are trained on the procedures, processes, and supporting technologies used to conduct vulnerability assessments.	❒	❒	
5.6.6.04 Activity: Vulnerability assessments are performed on incident management systems and networks.	❒	❒	
5.6.6.05 Activity: A list of POCs is maintained for notification and alert based on the results of vulnerability assessments.	❒	❒	
5.6.6.06 Activity: Information on vulnerability assessment is tracked and recorded.	❒	❒	
5.6.6.07 Activity: Remediation, response, and recovery solutions are implemented to address findings in the results of vulnerability assessments.	❒	❒	
Recommended Best Practices			
5.6.6.08 Activity: Lessons learned from vulnerability assessments are incorporated into vulnerability assessment processes, training, and testing.	❒	❒	
5.6.6.09 Control: Documented policies exist that define reporting requirements.	❒	❒	
5.6.6.10 Activity: Sources for tools and information used in vulnerability scanning are reviewed by vulnerability assessment personnel to ensure tools and information are up to date.	❒	❒	

5.6.6.11 Activity: Vulnerabilities found and remediated are handled through organizational change management mechanisms.	❒	❒	
5.6.6.12 Quality: A designated schedule is followed for performing vulnerability assessments (or more often as warranted).	❒	❒	
Institutional and Quality Improvement			
5.6.6.13 Control: Documented procedures exist that describe the process and method by which vulnerability assessments are conducted.	❒	❒	
5.6.6.14 Control: Documented procedures exist that describe how to report the results of the vulnerability assessments.	❒	❒	
5.6.6.15 Quality: Personnel are aware of, knowledgeable of, and consistently follow the procedures, processes, and methodologies for performing this task.	❒	❒	
5.6.6.16 Quality: A process and criteria (including timeliness, completeness, adequacy, and frequency of vulnerability assessments) exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	
5.6.6.17 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒	
Not Applicable		❒	**Not Observed**	❒	
Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes

Suggestions for Improvement
Implement automated tools for performing vulnerability scanning and tracking, including a vulnerability database that allows tracking of vulnerabilities by the incident management component or group and tracking of vulnerability remediation.

5.6 IM INFORMATION SYSTEMS

5.6.7 A patch management program is in place for the incident management systems.

Priority I

Clarification

This intent of this capability is to determine whether defined processes exist for patch management for incident management systems. These processes should include

- receiving alerts about patches
- testing patches
- installing patches
- monitoring installation to ensure patches were correctly installed on incident management systems and networks
- determining how to handle any exceptions or extensions when patching cannot be implemented immediately

Patch management records can also provide a source mechanism for trend analysis. It may not always be possible to patch a system or conduct sufficient testing to ensure a patch will work as expected on that system. Incident management personnel need to know which systems fall into these categories. They also need to ensure that the appropriate actions are taken to prevent patches from affecting operational production systems and that appropriate mitigation actions are taken to monitor and defend unpatched systems. Timely patch alerts and installation provide a method of protecting systems from threats. Patch management can help increase the organization's security posture by protecting critical incident management systems, networks, and data.

Team Guidance

The team should determine whether incident management personnel or another group within the organization has authority to install the patches on the incident management systems. Whoever has authority for performing patch management should be the group that is assessed for this capability.

The team should look for evidence that patch management personnel seek information about patch notifications from as many sources as needed, including US-CERT; software and hardware vendors; other vulnerability analysis and reporting organizations; and other security experts. These personnel should know or have access to information about which IM systems can and cannot be patched, and the associated rationale and mitigation. For example the IM function may have test devices, labs, or honeynet devices that they do not want to patch.

References

Regulatory References: None

[indirect]

FISMA 3544 *Federal agency responsibilities* (b)(3) [OLRC 2003]

"(b) AGENCY PROGRAM—Each agency shall develop, document, and implement an agency-wide information security program […] to provide information security for the information and information systems that support the operations and assets of the agency […] that includes—

(3) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate […]"

A Roadmap for Cybersecurity Research [DHS 2009]

"The Configuration and Patch Management domain is addressed primarily as a subset of the CM family of controls in SP 800-53."

Guidance References:

NIST SP 800-40 Ver. 2 *Creating a Patch and Vulnerability Management Program* [Mell 2005a]

"This publication is designed to assist organizations in implementing security patch and vulnerability remediation programs. It focuses on how to create an organizational process and test the effectiveness of the process. It also seeks to inform the reader about the technical solutions that are available for vulnerability remediation."

NIST SP 800-53 Rev. 4 *Security and Privacy Controls for Federal Information Systems and Organizations* [NIST 2013]

"SI-2 FLAW REMEDIATION

Control: The organization:

(a.) Identifies, reports, and corrects information system flaws;

(b.) Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;

(c.) Installs security-relevant software and firmware updates within [*Assignment: organization-defined time period*] of the release of the updates; and

(d.) Incorporates flaw remediation into the organizational configuration management process."

Organization Response

Examples of Evidence Sought

- ❑ Demonstration of automated tools for distributing and installing patches on incident management systems and networks
- ❑ Copies of reports sent to intermediate organization group as appropriate
- ❑ Confirmation receipts (for patches) from other entities when applicable
- ❑ Notification lists for any management or personnel to be contacted
- ❑ Mechanism for reporting and recording patch compliance and notification
- ❑ Guidance for patch installation
- ❑ Communication mechanisms for patch notification

Scoring Criteria	Yes	No	Evidence
Required			
5.6.7.01 Control: An up-to-date inventory exists of systems that cannot be patched due to operational, compliance, or other reasons.	❒	❒	
5.6.7.02 Control: A documented, up-to-date policy for patch management of IM systems exists, including assigned roles and responsibilities.	❒	❒	
5.6.7.03 Control: Personnel are trained on relevant technology.	❒	❒	
5.6.7.04 Control: Documentation exists for patch extension requests, describes the rationale, and identifies potential technical risks and mitigation strategies.	❒	❒	
5.6.7.05 Activity: The IM function is on the organizational notification patch list.	❒	❒	
5.6.7.06 Activity: Vulnerability and patch information is analyzed to determine if the information is relevant to incident management systems and networks.	❒	❒	
5.6.7.07 Activity: Patches are downloaded from a trusted, approved, or authorized site.	❒	❒	
5.6.7.08 Activity: Patches are tested using a test server or testbed where patches can be loaded and tested (checksums are verified, patches are proven not to cause failures, etc.).	❒	❒	
5.6.7.09 Activity: Patches are installed according to organizational guidelines.	❒	❒	
5.6.7.10 Activity: System vulnerabilities that cannot be patched are mitigated in an alternative way according to organizational guidance.	❒	❒	
5.6.7.11 Activity: Processes are in place to monitor, analyze, and conduct remediation on unpatched incident management systems.	❒	❒	
5.6.7.12 Activity: Processes are in place to monitor systems that cannot be patched.	❒	❒	

Recommended Best Practices			
5.6.7.13 Activity: Patch implementation reports are generated for incident management systems.	❒	❒	
5.6.7.14 Activity: The organization uses a cost-effective means of meeting patch compliance requirements (e.g., automated tools, templates, forms, data collection mechanisms).	❒	❒	
5.6.7.15 Activity: A searchable archive exists where patch notifications (alerts, bulletins, and advisories) are stored securely.	❒	❒	
Institutional and Quality Improvement			
5.6.7.16 Control: Documented procedures exist for patch management and testing.	❒	❒	
5.6.7.17 Quality: Personnel are aware of, knowledgeable of, and consistently follow the procedures and processes for performing this task.	❒	❒	
5.6.7.18 Quality: A process and criteria exist for evaluating how well this activity is performed and the quality of its artifacts.	❒	❒	
5.6.7.19 Quality: The quality and effectiveness of this activity are evaluated at least annually, and appropriate improvements are made.	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒
Not Applicable		❒	**Not Observed**	❒

Evidence Collected					
Document Review		Interviews		Direct Observation	

Notes
Suggestions for Improvement
None

5.6 IM INFORMATION SYSTEMS

5.6.8 More than one communications system or mechanism (other than email) exists for receiving and distributing notifications, information about new viruses, incidents, vulnerabilities, threats, and other kinds of warnings.

Priority II

Clarification

The intent of this capability is to measure the organization's ability to contact all relevant parties whenever necessary. Communication channels can fail in unexpected ways. As a proactive measure, an alternative means of communication must be established and tested to ensure proper communication during emergencies or time-critical activities.

Team Guidance

The team should look for documented policies, procedures, and guidance for implementing or maintaining alternate communication systems, as well as other evidence that such alternative communication channels exist (e.g., demonstrations). It is not sufficient for the primary and alternate means of communication (e.g., email servers, alternate systems) to be on the same network or connected in any other way that would create a single point of failure.

References

Regulatory References:

OMB Cir A-130 *Memorandum for Heads of Executive Departments and Agencies* App III

> "d) Contingency Planning. Establish and periodically test the capability to perform the agency function supported by the application in the event of failure of its automated support."

"National Security and Homeland Security Presidential Directive: National Continuity Policy

NATIONAL SECURITY PRESIDENTIAL DIRECTIVE/NSPD 51

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE/HSPD-20

This directive establishes a comprehensive national policy […]"

Guidance References:

NIST SP 800-61 Rev 2 *Computer Security Incident Handling Guide* [Cichonski 2012]

> "Sec 3.2.7 Incident Notification
> When an incident is analyzed and prioritized, the incident response team needs to notify the appropriate individuals so that all who need to be involved will play their roles."

NIST SP 800-34 Rev 1 *Contingency Planning Guide for Federal Information Systems* [Swanson 2010]

NIST SP 800-53 Rev 4 *Security and Privacy Controls for Federal Information Systems and Organizations* [NIST 2013]

> "Contingency Planning
>
> […] CP-8 Telecommunications Services

CP-9 Information System Backup

CP-10 Information System Recovery and Reconstitution

CP-11 Alternate Communication Protocols

CP-12 Safe Mode

CP-13 Alternative Security Mechanisms"

[indirect]

DHS Federal Continuity Directive 1: Federal Executive Branch National Continuity Program and Requirements: Annex C [DHS 2008a]

"ANNEX C. BUDGETING AND ACQUISITION OF RESOURCES

Agencies must identify the people, communications, facilities, infrastructure, and transportation requirements, which are necessary to the successful implementation and management of an agency's continuity program."

DHS Federal Continuity Directive 2: Federal Executive Branch Mission Essential Function and Primary Mission Essential Function Identification and Submission Process [DHS 2008b]

"This Federal Continuity Directive (FCD) implements the requirements of Federal Continuity Directive 1, ANNEX C. It provides guidance and direction to Federal executive branch departments and agencies for identification of their Mission Essential Functions (MEFs) and potential Primary Mission Essential Functions (PMEFs). It includes guidance and checklists to assist departments and agencies in assessing their essential functions through a risk management process and in identifying potential PMEFs that support the National Essential Functions (NEFs)—the most critical functions necessary to lead and sustain the nation during a catastrophic emergency."

Organization Response

Examples of Evidence Sought

- ❑ Demonstration of alternate communication paths (e.g., secure phone, secure email, alternate email account(s) on separate networks, and secure webpage for emergency communications, Twitter, RSS, satellite phones, radios, etc.)
- ❑ Contact lists with alternate contact information for designated personnel
- ❑ Procedures for using alternate communication paths
- ❑ Contingency or COOP plan that describes alternative communication paths and when to use them

Scoring Criteria	Yes	No	Evidence
Required			
5.6.8.01 Control: There is a documented plan or guidance for when to use alternative communication paths and how they are set up and maintained.	❒	❒	

5.6.8.02 Control: Documented guidance exists for each type of communication method.	❒	❒	
5.6.8.03 Control: Personnel are appropriately trained on the alternative communications process and supporting technologies.	❒	❒	
5.6.8.04 Activity: An alternate communications system and plan for its operation are maintained and tested.	❒	❒	
5.6.8.05 Activity: Alternate communication mechanisms are used successfully when normal mechanisms are unavailable.	❒	❒	
5.6.8.06 Activity: The incident management COOP includes an alternate means of communications.	❒	❒	
Recommended Best Practices			
5.6.8.07 Quality: More than one alternate communication method exists.	❒	❒	
5.6.8.08 Quality: Defined criteria exist, including when to implement alternate methods.	❒	❒	
Institutional and Quality Improvement			
5.6.8.09 Control: Documented procedures exist that define when and how to use the alternate communication channels and equipment.	❒	❒	
5.6.8.10 Quality: Personnel are aware of, knowledgeable of, and consistently follow or use the procedures, processes, methodologies, and technologies for performing this task.	❒	❒	
5.6.8.11 Quality: Periodic testing and evaluation of communications availability is performed (e.g., monthly, semi-annually, when service providers change).	❒	❒	

Scoring	**Met (all Required indicators have Yes answers)**	❒	**Not Met (one or more Required indicators have a No answer)**	❒
Not Applicable		❒	**Not Observed**	❒

Evidence Collected					
Document Review		Interviews		Direct Observation	
Notes					
Suggestions for Improvement					
None					

Appendix A: List of Incident Management Capabilities

This appendix contains a simple list of all the capability statements contained in this document. It is provided for convenience for those who want a complete list.

Capabilities	Priority
Prepare	
Establish IM Function	
1.1.1 An incident management function or CSIRT has been officially designated by the organization head or chief information officer (CIO).	II
1.1.2 An incident management plan has been developed and implemented for the organization.	I
1.1.3 Roles and responsibilities are documented for key incident management activities throughout the organization and followed.	I
1.1.4 Formal interfaces for conducting organizational incident management activities are defined and maintained.	I
1.1.5 Trusted relationships are maintained with experts who can give technical and nontechnical advice and information.	III
Core Processes and Tools	
1.2.1 A communication plan for incident management activities has been established and disseminated.	II
1.2.2 An IM information management plan is established and followed.	II
1.2.3 An inventory exists of mission-critical systems and data.	I
1.2.4 Workflow management processes and/or systems are implemented.	III
1.2.5 A central repository exists for recording and tracking security events and incidents.	I
1.2.6 Security events and incidents are categorized and prioritized according to organizational guidance.	II
1.2.7 An insider threat program exists within the organization.	I

Capabilities	Priority
Protect	
Risk Assessment	
2.1.1 Security risk assessments (RAs) are performed on the constituents' organization.	I
2.1.2 The constituents get help correcting problems identified through security risk assessment (RA) activities.	II
Prevention	
2.2.1 The organization has an institutionalized malware prevention program.	I
Operational Exercises for Incident Management	
2.3.1 Operational exercises are conducted to assess the IM function of the organization.	II
Training and Guidance	
2.4.1 Guidance is provided to constituents on best practices for protecting their systems and networks.	II
2.4.2 Constituents are provided with security education, training, and awareness (ETA).	I
Vulnerability Management	
2.5.1 A patch management and alert program exists.	I
2.5.2 Proactive vulnerability assessment is performed on constituent networks and systems.	I
2.5.3 Constituents receive help to correct problems identified by vulnerability assessment activities.	II
Detect	
Network and Systems Security Monitoring	
3.1.1 Security monitoring is continuously performed on all constituent networks and systems.	I
External Sources of Incident Information	

Capabilities	Priority
3.2.1 Events and incidents are reported from outside the organization.	I
Threat and Situational Awareness	
3.3.1 Public monitoring of external security websites and other trusted sources of information is conducted.	I
3.3.2 Trend analysis is supported and conducted.	II
3.3.3 Network and system configurations or rule sets are reviewed and updated in response to changes in the threat environment, and constituents are notified of the updates.	I
3.3.4 Penetration testing is conducted on organizational networks and systems.	I
Respond	
Incident Reporting	
4.1.1 Events and incidents are reported from the constituency.	I
4.1.2 Incidents are reported to appropriate management in accordance with organizational guidelines.	I
4.1.3 Incidents are reported to and coordinated with the appropriate external organizations or groups in accordance with organizational guidelines.	I
4.1.4 Incident management is supported for restricted information, networks, and systems.	I
Analysis	
4.2.1 Incident management personnel conduct triage of events and incidents.	I
4.2.2 Incident analysis is performed on declared incidents.	I
4.2.3 Incident correlation is performed to identify similar activity.	II
4.2.4 Impact of an incident is determined.	II
4.2.5 Incident root cause analysis is conducted.	II
4.2.6 Fusion analysis is performed to identify concerted attacks and shared vulnerabilities.	III

Capabilities		Priority
4.2.7	Retrospective analysis is conducted.	III
4.2.8	Media analysis is performed on constituent networks and systems.	II
4.2.9	Artifact or malware analysis is conducted.	II
Incident Response		
4.3.1	General incident response guidance and procedures are distributed to constituents.	II
4.3.2	Incidents are resolved.	I
4.3.3	Incident management personnel coordinate incident response across stakeholders.	I
4.3.4	Incident management personnel create alerts and warnings, and distribute them as needed.	I
4.3.5	Incident management personnel verify that a response is implemented, as appropriate, and that the incident is closed, in accordance with organizational guidance.	I
4.3.6	Postmortem reviews of significant incidents are conducted, and lessons learned are identified and acted upon, as appropriate.	I
Sustain		
MOUs and Contracts		
5.1.1	A list of incident management services provided by the designated incident management function is documented.	II
5.1.2	The constituency provides advance notification of all changes or planned outages to their networks.	III
5.1.3	Formal agreements exist for managing IM activities with third parties across the supply chain.	I
Project/Program Management		
5.2.1	A financial plan exists for incident management activities.	III
5.2.2	A workforce plan exists for incident management personnel.	II
5.2.3	A personnel security plan exists for incident management personnel.	I

Capabilities		Priority
5.2.4	A quality assurance (QA) program exists to ensure the quality of provided products and services.	II
5.2.5	An established plan exists to ensure continuity of operations for incident management.	I
5.2.6	The effectiveness of the incident management function in meeting its mission is routinely evaluated and improved.	III
IM Technology Development, Evaluation, and Implementation		
5.3.1	The incident management function has the tools it needs to meet its mission.	I
5.3.2	Software tools are tested for use within the incident management environment.	II
5.3.3	The IT infrastructure for incident management is adequate to support incident management operations.	I
Personnel		
5.4.1	A training program exists for incident management personnel.	I
5.4.2	Support for professional development exists for incident management personnel.	III
Security Administration		
5.5.1	Physical protective measures are in place to protect incident management IT systems, facilities, and personnel.	I
5.5.2	An operations security (OPSEC) program exists.	I
IM Information Systems		
5.6.1	An inventory exists of mission-critical incident management systems, data, and information.	I
5.6.2	Defense-in-depth strategies and methodologies exist for hardening the incident management computer networks and systems.	I
5.6.3	Processes and technologies exist to support the confidentiality, integrity, and availability of incident management data and information.	I
5.6.4	Network security monitoring is performed on all incident-management-related networks and systems.	I
5.6.5	Security risk assessments (RAs) are performed on the incident management function.	I

Capabilities		Priority
5.6.6	Vulnerability assessments are performed on incident management systems and networks.	I
5.6.7	A patch management program is in place for the incident management systems.	I
5.6.8	More than one communications system or mechanism (other than email) exists for receiving and distributing notifications, information about new viruses, incidents, vulnerabilities, threats, and other kinds of warnings.	II

Appendix B: Acronyms

A&O	analysis and operations
ACL	access control list
ADS	anomaly detection system
A/V	audio/video
AV	anti-virus
AVS	anti-virus software
C&A	certification and accreditation
CAESARS	Continuous Asset Evaluation, Situational Awareness, and Risk Scoring Reference Architecture Report
CBK	Common Body of Knowledge
CBT	computer-based training
CCV	Cybersecurity Capabilities Validation
CD	compact disc
CERT/CC	CERT Coordination Center
CIA	confidentiality, integrity, and availability
CIO	chief information officer
CISO	chief information security officer
CISSP	Certified Information Systems Security Professional
CM	continuous monitoring
CMMI	Capability Maturity Model Integration
CMU	Carnegie Mellon University
CND	computer network defense
CNDSP	computer network defense service provider
COBIT	Control Objectives for Information and related Technology
CONOPS	concept of operations
COOP	continuity of operations
COP	common operational picture
CP	contingency planning
CSIRT	computer security incident response team
CVE	Common Vulnerabilities and Exposures
D/A	department/agency
DDOS	distributed denial of service
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DMZ	demilitarized zone
DNS	domain name system
DoD	Department of Defense

DoS	denial of service
ETA	education, training, and awareness
F-CND	Federal-Computer Network Defense
FAX	facsimile
FCD	Federal Continuity Directive
FCMR	Federal Cybersecurity Maturity Roadmap
FE	framework extension
FFIEC	Federal Financial Institutions Examination Council
FIPS	Federal Information Processing Standards
FIRST	Forum of Incident Response and Security Teams
FISMA	Federal Information Security Management Act of 2002
FNR	Federal Network Resilience
FNS	Federal Network Security
FOUO	for official use only
FYI	for your information
GFIRST	Government Forum of Incident Response and Security Teams
GnuPG	GNU Privacy Guard
GRS	General Records Schedule
HR	human resources
IA	information assurance
IC	intelligence community
IDPS	Intrusion Detection and Prevention System
IDS	intrusion detection system
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IG	inspector general
IM	incident management
IMF	Incident Management Function
IP	internet protocol
IPS	intrusion prevention system
IR	incident response
ISAC	Information Sharing and Analysis Center
$(ISC)^2$	International Information Systems Security Certification Consortium
ISCM	information system continuous monitoring
ISCP	Information System Contingency Plan
ISF	Information Security Forum
ISO	information security officer OR International Organization for Standardization
ISP	internet service provider

IT	information technology
ITGI	Information Technology Governance Institute
ITIL	IT Infrastructure Library
JWICS	Joint Worldwide Intelligence Communications System
LE	law enforcement
LOA	letter of agreement
MEF	mission essential function
MIME	Multipurpose Internet Mail Extensions
MO	modus operandi (mode of operation)
MOA	memorandum of agreement
MOU	memorandum of understanding
MSSP	managed security service provider
NARA	National Archives and Records Administration
NDA	non-disclosure agreement
NEF	national essential function
NFAT	network forensics analysis tools
NIC	network information center
NIST	National Institute of Standards and Technology
NIST SP	NIST Special Publication
NITTF	National Insider Threat Task Force
NOC	network operations center
NSA	National Security Agency
NVD	National Vulnerability Database
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
OGC	Office of Government Commerce
OLRC	Office of the Law Revision Counsel
OMB	Office of Management and Budget
OPSEC	operations security
OS	operating system
PC	personal computer
PE	physical and environmental
PGP	Pretty Good Privacy
PII	personally identifiable information
PKI	public key infrastructure
PMEF	primary mission essential function
POC	point of contact
QA	quality assurance
RA	risk assessment
RDF	resource description framework

RFC	request for comments
RSS	RDF Site Summary
SA	situational awareness
SCIF	Sensitive Compartment Information Facility
SDLC	system development lifecycle
SEI	Software Engineering Institute
SEIM	security event and incident management
SIPRNET	Secret Internet Protocol Router Network
SKiP	Security Knowledge in Practice
SLA	service level agreement
S/MIME	Secure/Multipurpose Internet Mail Extensions
SME	subject matter expert
SMS	short message service
SOC	security operations center
SOP	standard operating procedure
SP	special publication
SSP	system security plan
STE	secure terminal equipment
SWO	senior watch officer
TERENA	Trans-European Research and Education Networking Association
TICAP	Trusted Internet Connection Access Provider
TS	top secret
TT&E	testing, training, and exercise
US-CERT	United States Computer Emergency Readiness Team
VPN	virtual private network
VS	vulnerability scanning
XML	Extensible Markup Language

Appendix C: Bibliography

URLs are valid as of the publication date of this document.

[Alberts 2004]
Alberts, Chris; Dorofee, Audrey; Killcrece, Georgia; Ruefle, Robin; & Zajicek, Mark. *Defining Incident Management Processes for CSIRTs: A Work in Progress.* CMU/SEI-2004-TR-015 ADA453378. Software Engineering Institute, Carnegie Mellon University. 2004. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=7153

[Alberts 2013]
Alberts, Chris; Dorofee, Audrey; Ruefle, Robin; & Zajicek, Mark. *An Introduction to the Mission Risk Diagnostic for Incident Management Capabilities (MRD-IMC).* CMU/SEI-2013-TN-015. Software Engineering Institute, Carnegie Mellon University. 2013. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=91452

[Barker 2003]
Barker, William C. *Guideline for Identifying an Information System as a National Security System* (NIST Special Publication 800-59). 2003. http://csrc.nist.gov/publications/nistpubs/800-59/SP800-59.pdf

[Cichonski 2012]
Cichonski, Paul; Millar, Tom; Grance, Tim; & Scarfone, Karen. *Computer Security Incident Handling Guide* (NIST Special Publication 800-61, Rev 2). 2012. http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf

[Dempsey 2010]
Dempsey, Kelley; Sha Chawlaa, Nirali; Johnson, Arnold; Johnston, Ronald; Clay Jones, Alicia; Orebaugh, Angela; Scholl, Matthew; & Stine, Kevin. *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* (NIST Special Publication 800-137). 2010. http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf

[DHS 2008a]
Department of Homeland Security. *DHS Federal Continuity Directive 1: Federal Executive Branch National Continuity Program and Requirements: Annex C*. 2008. http://www.fema.gov/pdf/about/org/ncp/fcd1.pdf

[DHS 2008b]
Department of Homeland Security. *DHS Federal Continuity Directive 2: Federal Executive Branch Mission Essential Function and Primary Mission Essential Function Identification and Submission Process*. 2008. http://www.fema.gov/pdf/about/org/ncp/fcd2.pdf

[DHS 2009]
Department of Homeland Security. *A Roadmap for Cybersecurity Research*. 2009. https://www.dhs.gov/sites/default/files/publications/CSD-DHS-Cybersecurity-Roadmap.pdf

[DHS 2010]
Department of Homeland Security. Department of Homeland Security Federal Network Security Branch. *Continuous Asset Evaluation, Situational Awareness, and Risk Scoring Reference Architecture Report (CAESARS)*. 2010. https://csrc.nist.gov/csrc/media/publications/nistir/7756/draft/documents/draft-nistir-7756_second-public-draft.pdf

[DHS 2012a]
Department of Homeland Security. *Cybersecurity Capability Validation (CCV) Assessment Method and Process Guidance Version 1.1*. U.S Department of Homeland Security. 2012.

[DHS 2012b]
Department of Homeland Security. *IT Program Assessment: Department of Homeland Security (DHS) Analysis and Operations (A&O) Common Operating Picture (COP)*. U.S. Department of Homeland Security. 2012. http://www.dhs.gov/xlibrary/assets/mgmt/itpa-ao-cop2012.pdf

[Dorofee 2007]
Dorofee, Audrey; Killcrece, Georgia; Ruefle, Robin; & Zajicek, Mark. *Incident Management Capability Metrics, Version 0.1.* CMU/SEI-2007-TR-008 ADA468688. Software Engineering Institute, Carnegie Mellon University. 2007. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8379

[ENISA 2006]
ENISA. *CSIRT A Step-by-Step Approach on How to Set Up a CSIRT.* 2006. https://www.enisa.europa.eu/publications/csirt-setting-up-guide

[ENISA 2010]
ENISA. *CSIRT Good Practice Guide for Incident Management.* 2010. https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management

[FFIEC 2006]
Federal Financial Institutions Examination Council (FFIEC). *IT Examination Handbook InfoBase*. 2006. http://ithandbook.ffiec.gov/

[Grance 2006]
Grance, Tim; Nolan, Tamara; Burke, Kristin; & Good, Travis. *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities* (NIST Special Publication 800-84). 2006. http://csrc.nist.gov/publications/nistpubs/800-84/SP800-84.pdf

[Hash 2005]
Hash, Joan; Bartol, Nadya; Rollins, Holly; Robinson, Will; Abeles, John; & Batdorff, Steve. *Integrating IT Security into the Capital Planning and Investment Control Process* (NIST Special Publication 800-65). 2005. http://csrc.nist.gov/publications/nistpubs/800-65/SP-800-65-Final.pdf

[ISC^2 2007]
International Information Systems Security Certification Consortium (ISC)^2. *Certified Information Systems Security Professional (CISSP) Common Body of Knowledge (CBK).* 2007. http://www.isc2.org/official-isc2-textbooks.aspx

[ISF 2012]
Information Security Forum. *The Standard of Good Practice for Information Security*. 2012. https://www.securityforum.org/tool/the-isf-standardrmation-security/

[ISO 2005a]
International Organization for Standardization. *Information technology — Security techniques — Information security management systems—Requirements* (ISO/IEC 27001:2005). 2005. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103

[ISO 2005b]
International Organization for Standardization. *Information technology — Security techniques — Code of practice for information security management* (ISO/IEC 27002:2005) 2005. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297

[ITGI 2012]
IT Governance Institute. *Control Objectives for Information and related Technology (COBIT) 5*. 2012. http://www.isaca.org/cobit

[Johnson 2011]
Johnson, Arnold; Dempsey, Kelley; Ross, Ron; Gupta, Sarbari; & Bailey, Dennis. *Guide for Security-Focused Configuration Management of Information Systems* (NIST Special Publication 800-128). 2011. http://csrc.nist.gov/publications/nistpubs/800-128/sp800-128.pdf

[JTFTI 2012]
Joint Task Force Transformation Initiative. *Guide for Conducting Risk Assessments* (NIST Special Publication 800-30 Rev 1). 2012. http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

[Kent 2006a]
Kent, Karen & Souppaya, Murugiah. *Guide to Computer Security Log Management* (NIST Special Publication 800-92). 2006. http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf

[Kent 2006b]
Kent, Karen; Chevalier, Suzanne; Grance, Tim; & Dang, Hung. *Guide to Integrating Forensic Techniques into Incident Response* (NIST Special Publication 800-86). 2006. http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf

[Killcrece 2003a]
Killcrece, Georgia; Kossakowski, Klaus-Peter; Ruefle, Robin; & Zajicek, Mark. *State of the Practice of Computer Security Incident Response Teams (CSIRTs).* CMU/SEI-2003-TR-001, ADA421664. Software Engineering Institute, Carnegie Mellon University. 2003. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6571

[Killcrece 2003b]
Killcrece, Georgia; Kossakowski, Klaus-Peter; Ruefle, Robin; & Zajicek, Mark. *Organizational Models for Computer Security Incident Response Teams (CSIRTs).* CMU/SEI-2003-HB-001, ADA421684. Software Engineering Institute, Carnegie Mellon University. 2003. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6295

[Killcrece 2002]
Killcrece, Georgia; Kossakowski, Klaus-Peter; Ruefle, Robin; & Zajicek, Mark. *CSIRT Services*. Software Engineering Institute, Carnegie Mellon University. 2002. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=53046

[Mell 2012]
Mell, Peter; Waltermire, David; Feldman, Larry; Booth, Harold; Ragland, Zach; Ouyang, Alfred; & McBride, Timothy. *CAESARS Framework Extension: An Enterprise Continuous Monitoring Technical Reference Architecture (Second Draft).* 2012. http://csrc.nist.gov/publications/drafts/nistir-7756/Draft-NISTIR-7756_second-public-draft.pdf

[Mell 2005a]
Mell, Peter; Bergeron, Tiffany; & Henning, David. *Creating a Patch and Vulnerability Management Program* (NIST Special Publication 800-40, Version 2.0). 2005. http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf

[Mell 2005b]
Mell, Peter; Kent, Karen; & Nusbaum, Joseph. *Guide to Malware Incident Prevention and Handling* (NIST Special Publication 800-83). 2005. http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf

[NARA 2010]
The National Archives and Records Administration. *General Records Schedule 24—Information Technology Operations and Management Records*. 2010. https://www.archives.gov/files/records-mgmt/grs/grs24.pdf

[NIST 2004]
National Institute of Standards and Technology. *Standards for Security Categorization of Federal Information and Information Systems* (FIPS PUB 199). 2004. http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

[NIST 2006]
National Institute of Standards and Technology. *Minimum Security Requirements for Federal Information and Information Systems* (FIPS PUB 200). 2006. http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

[NIST 2009a]
National Institute of Standards and Technology, Joint Task Force Transformation Initiative. *Recommended Security Controls for Federal Information Systems and Organizations* (NIST Special Publication 800-53, Rev 3). 2009. http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

[NIST 2009b]
National Institute of Standards and Technology. *NIST Special Publications, 800 Series*. 2009. http://csrc.nist.gov/publications/PubsSPs.html

[NIST 2010a]
National Institute of Standards and Technology, Joint Task Force Transformation Initiative. *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Lifecycle Approach* (NIST Special Publication 800-37 Rev 1). 2010. http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

[NIST 2010b]
National Institute of Standards and Technology, Joint Task Force Transformation Initiative. *Guide for Assessing the Security Controls in Federal Information Systems* (NIST Special Publication 800-53A Rev 1). 2010. http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf

[NIST 2011]
National Institute of Standards and Technology, Joint Task Force Transformation Initiative. *Managing Information Security Risk: Organization, Mission, and Information System View* (NIST Special Publication 800-39). 2011. http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

[NIST 2012]
National Institute of Standards and Technology. *Computer Security Incident Handling Guide (Draft)* (NIST Special Publication 800-61 Rev 2 DRAFT). 2012. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

[NIST 2013]
National Institute of Standards and Technology. *Security and Privacy Controls for Federal Information Systems and Organizations* (NIST Special Publication 800-53 Rev 4). 2013. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

[NWG 1998]
Network Working Group. *Expectations for Computer Security Incident Response*. 1998. http://www.ietf.org/rfc/rfc2350.txt

[OGC 2006]
Office of Government Commerce. *IT Infrastructure Library (ITIL).* 2006. http://www.itil-officialsite.com/

[OLRC 2003]
Office of the Law Revision Counsel, U.S. House of Representatives. United States Code, Title 44, Sections 3541-3549 "Federal Information Security Management Act of 2002." 2003. http://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title44-chapter35-front&num=0&edition=prelim

[OMB 1996]
Office of Management and Budget. *Circular No. A-130, Revised, Appendix III, Security of Federal Automated Information Resources.* 1996. https://a130.cio.gov/appendix3/

[OMB 2007]
Office of Management and Budget. *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (memorandum). 2007. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2007/m07-16.pdf

[Reid 2004]
Reid, Gavin & Schieber, Dustin. *CSIRT Case Classification (Example for Enterprise CSIRT).* 2004. https://www.first.org/resources/guides/#CSIRT-Case-Classification-Example-for-enterprise-CSIRT

[Ross 2004]
Ross, Ron; Swanson, Marianne; Stoneburner, Gary; Katzke, Stu; & Johnson, Arnold. *Guide for the Security Certification and Accreditation of Federal Information Systems* (NIST Special Publication 800-37) 2004. https://security.health.ufl.edu/VA_Research/NIST%20800-37-Security%20Cert%20and%20Accred%20for%20FIS.pdf

[Scarfone 2007]
Scarfone, Karen & Mell, Peter. *Guide to Intrusion Detection and Prevention Systems (IDPS)* (NIST Special Publication 800-94). 2007. http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

[Scarfone 2008]
Scarfone, Karen; Souppaya, Murugiah; Cody, Amanda; & Orebaugh, Angela. *Technical Guide to Information Security Testing and Assessment* (NIST Special Publication 800-115). 2008. http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

[Scarfone 2009]
Scarfone, Karen & Hoffman, Paul. *Guidelines on Firewalls and Firewall Policy* (NIST Special Publication 800-41, Rev 1). 2009. https://csrc.nist.gov/publications/detail/sp/800-41/rev-1/final

[Sharp 2001]
Sharp, Alec & McDermott, Patrick. *Workflow Modeling: Tools for Improvement and Application Development*. Boston, MA: Artech House. 2001. http://www.artechhouse.com/Main/Books/Workflow-Modeling-Tools-for-Process-Improvement-an-1298.aspx

[SEI 2003]
Software Engineering Institute. *Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)*. Software Engineering Institute, Carnegie Mellon University. 2003. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=309051

[SEI 2010a]
CMMI Product Team. *CMMI for Development, Version 1.3*. CMU/SEI-2010-TR-033. Software Engineering Institute, Carnegie Mellon University. 2010. http://www.sei.cmu.edu/library/abstracts/reports/10tr033.cfm

[SEI 2010b]
CMMI Product Team. *CMMI for Services, Version 1.3*. Software Engineering Institute, Carnegie Mellon University. 2010. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=9661

[Stine 2008]
Stine, Kevin; Kissel, Rich; Barker, William C.; Fahlsing, Jim; & Gulick, Jessica. *Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories* (NIST Special Publication 800-60 Rev 1). 2008. http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf

[Swanson 1996]
Swanson, Marianne & Guttman, Barbara. *Generally Accepted Principles and Practices for Securing Information Technology Systems* (NIST Special Publication 800-14). 1996. http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf

[Swanson 2006]
Swanson, Marianne; Hash, Joan; & Bowen, Pauline. *Guide for Developing Security Plans for Federal Information Systems* (NIST Special Publication 800-18, Rev 1). 2006. http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf

[Swanson 2010]
Swanson, Marianne; Bowen, Pauline; Wohl Phillips, Amy; Gallup, Dean; & Lynes, David. *Contingency Planning Guide for Federal Information Systems* (NIST Special Publication 800-34, Rev 1). 2010. http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

[Tracy 2007]
Tracy, Miles; Jansen, Wayne; Scarfone, Karen; & Butterfield, Jason. *Guidelines on Electronic Mail Security* (NIST Special Publication 800-45 Version 2). 2007. http://csrc.nist.gov/publications/nistpubs/800-45-version2/SP800-45v2.pdf

[West-Brown 2003]
West-Brown, Moira J.; Stikvoort, Don; Kossakowski, Klaus-Peter; Killcrece, Georgia; Ruefle, Robin; & Zajicek, Mark. *Handbook for Computer Security Incident Response Teams (CSIRTs)* (CMU/SEI-2003-HB-002, ADA413778). Software Engineering Institute, Carnegie Mellon University. 2003. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6305

[Wilson 2003]
Wilson, Mark & Hash, Joan. *Building an Information Technology Security Awareness and Training Program* (NIST Special Publication 800-50). 2003. http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	December 2018	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Incident Management Capability Assessment	FA8702-15-D-0002

6. AUTHOR(S)

Audrey Dorofee, Robin Ruefle, Mark Zajicek, David McIntire, Christopher Alberts, Samuel Perl, Carly Lauren Huth, Pennie Walters

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2018-TR-007

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
SEI Administrative Agent AFLCMC/AZS 5 Eglin Street Hanscom AFB, MA 01731-2100	

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

Successful management of incidents that threaten an organization's computer security is a complex endeavor. Frequently an organization's primary focus is on the response aspects of security incidents, which results in its failure to manage incidents beyond simply reacting to threatening events.

The capabilities presented in this document are intended to provide a baseline or benchmark of incident management practices for an organization. The incident management capabilities—provided in a series of statements and indicators—define the actual benchmark. The capabilities explore different aspects of incident management activities for preparing or establishing an incident management function; protecting, detecting, and responding to unauthorized activity in an organization's information systems and computer networks; and sustaining the ability to provide those services. This benchmark can be used by an organization to assess its current incident management function for the purpose of process improvement. This assessment will also help assure system owners, data owners, and operators that their incident management services are being delivered with a high standard of quality and success within acceptable levels of risk.

14. SUBJECT TERMS	15. NUMBER OF PAGES
incident management, incident management capabilities	351

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. Z39-18
298-102