



## 5-Incident Management

### Cybersecurity Assessment Tool for Transit (CATT) Welcome

The Cybersecurity Assessment Tool for Transit (CATT) is designed to provide transit agencies with an on-ramp to begin identifying and building foundational elements of a cybersecurity program. CATT incorporates the guidance of the Cyber Resilience Review (CRR) and the National Institute of Standards and Technology cybersecurity framework, but takes the additional steps of tailoring the assessment process to transit organizations that would benefit from more introductory materials and transit-aware guidance.

Each of the existing ten CRR Supplemental Resource Guides provides detailed guidance for the CRR process areas and are excellent assets for any transit organization building out the fundamentals of their cybersecurity practices. To complement CATT, each CRR Resource Guide has additional CATT- and transit-relevant resources from the American Public Transportation Association (APTA), Center for Internet Security (CIS), National Institute of Standards and Technology (NIST), and other beginner-friendly cyber resource guides.

Incident Management CATT Resources:

- The Mineta Transportation Institute (MTI) in 2019 published a [report](#) that includes a helpful breakdown of incident response by stakeholder and attack stage (see page 12 of MTI report).
  - Francoeur, Jacques R. Mineta Transportation Institute, 2019, *Managing Cyber Risks & Business Exposure in the Surface Transportation Ecosystem*, <https://transweb.sjsu.edu/sites/default/files/1739-Francoeur-Managing-Cyber-Risks-Transportation.pdf>. Accessed 26 Mar. 2022.



# **CRR Supplemental Resource Guide**



Volume 5

## **Incident Management**

Version 1.1

Copyright 2016 Carnegie Mellon University

This material is based upon work funded and supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of Department of Homeland Security or the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

CERT® and OCTAVE® are registered marks of Carnegie Mellon University.

DM-0003279

# Table of Contents

<b>I. Introduction .....</b>	<b>1</b>
Series Welcome.....	1
Audience.....	3
<b>II. Incident Management .....</b>	<b>3</b>
Overview.....	3
Detect Events .....	4
Triage and Analyze .....	5
Respond and Recover .....	5
Improve Capability .....	6
Develop a Plan .....	6
<b>III. Create an Incident Management Plan.....</b>	<b>8</b>
Before You Begin.....	8
Step 1. Obtain support for incident management planning. ....	9
Step 2. Establish an event detection process. ....	9
Step 3. Establish a triage and analysis process.....	11
Step 4. Establish an incident declaration process.....	12
Step 5. Establish an incident response and recovery process.....	13
Step 6. Establish an incident communications process. ....	15
Step 7. Establish a post-incident analysis and improvement process.....	18
Step 8. Assign roles and responsibilities for incident management. ....	19
Output of Section III .....	21
<b>IV. Test the Incident Management Plan.....</b>	<b>22</b>
Before You Begin.....	22
Step 1. Establish a testing process.....	22
Step 2. Test the incident management plan.....	23
Step 3. Record and report the results. ....	23
Output of Section IV .....	24
<b>V. Improve the Incident Management Plan .....</b>	<b>25</b>
Before You Begin.....	25
Step 1. Identify signs that the incident management plan needs to be revised, and make indicated improvements to the plan.....	25
Step 2. Conduct an after-action review of plan activities. ....	26
Output of Section V .....	27
<b>VI. Conclusion .....</b>	<b>28</b>
<b>Appendix A. Example Incident Management Plan Template.....</b>	<b>29</b>
<b>Appendix B. Example Cybersecurity Policy Template .....</b>	<b>34</b>
<b>Appendix C. Example Incident Declaration Criteria.....</b>	<b>36</b>
<b>Appendix D. Example Incident Reporting Template .....</b>	<b>38</b>
<b>Appendix E. CRR/CERT-RMM Practice/NIST CSF Subcategory Reference .....</b>	<b>44</b>
<b>Endnotes.....</b>	<b>47</b>





## I. Introduction

### Series Welcome

Welcome to the CRR Implementation Guide series. This document is 1 of 10 implementation guides developed by the Department of Homeland Security's (DHS) Cyber Security Evaluation Program (CSEP) to help organizations implement practices identified as considerations for improvement during a Cyber Resilience Review (CRR).<sup>1</sup> The CRR is an interview-based assessment that captures an understanding and qualitative measurement of an organization's *cyber resilience*. Cyber resilience is the organization's ability to adapt to risk that affects its core capacities.<sup>2</sup> It also highlights the organization's ability to manage operational risks to critical services and associated assets during normal operations and during times of operational stress and crisis. The guides were developed for organizations that have participated in a CRR, but any organization interested in implementing or maturing cyber resilience capabilities will find these guides useful.

The 10 domains covered by the CRR Implementation Guide series are

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

⇌ ***This guide***

Each implementation guide in this series has the same basic structure, but each can be used independently. Each guide focuses on the development of plans and artifacts that support the implementation and execution of operational resilience capabilities. Organizations using more than one implementation guide will be able to leverage complementary materials and suggestions to optimize their adoption approach. For example, this Incident Management guide suggests that a contact list be developed to support incident response. The information in that list can also be used as a starting point when developing the contact list recommended by the Service Continuity Management guide. Other examples of materials that can be leveraged between guides include the scoping of specific implementation activities and the identification of key stakeholders.

The objective of the CRR is to allow organizations to measure the performance of fundamental cybersecurity practices. DHS introduced the CRR in 2011. In 2014 DHS launched the Critical Infrastructure Cyber Community or C<sup>3</sup> (pronounced "C Cubed") Voluntary Program to assist the enhancement of critical infrastructure cybersecurity and to encourage the adoption of the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF). The NIST CSF provides a common taxonomy and mechanism for organizations to

1. describe their current cybersecurity posture
2. describe their target state for cybersecurity
3. identify and prioritize opportunities for improvement within the context of a continuous and repeatable process
4. assess progress toward the target state
5. communicate among internal and external stakeholders about cybersecurity risk

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

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

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

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

This guide is intended for organizations seeking help in establishing an incident management process and for organizations seeking to improve their existing incident management process. More specifically this guide

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

The guide is structured as follows:

- I. Introduction—Introduces the *CRR Implementation Guide* series and describes the content and structure of these documents.
- II. Incident Management—Presents an overview of the incident management process and establishes some basic terminology.
- III. Create an Incident Management Plan—Outlines a plan creation process and identifies issues and considerations to help ensure that the plan addresses the organization's needs.
- IV. Test the Incident Management Plan—Outlines the process and considerations for testing an incident management plan.

---

<sup>®</sup> CERT® is a registered mark owned by Carnegie Mellon University.

V. Improve the Incident Management Plan—Outlines the process and considerations for improving your incident management plan so that it continues to address your organization’s needs.

VI. Conclusion—Provides contacts and references for further information.

#### Appendices

- A. Example Incident Management Plan Template
- B. Example Cybersecurity Policy Template
- C. Example Incident Declaration Criteria
- D. Example Incident Reporting Template
- E. CRR/CERT-RMM Practice/NIST CSF Subcategory Reference

## Audience

The principal audience for this guide includes individuals responsible for managing or mitigating cybersecurity incidents, including executives who establish policies and priorities for incident management, managers and planners who are responsible for converting executive decisions into plans, and operations staff who implement the plans and participate in the response to cybersecurity incidents.

*To learn more about the source documents for this guide and for other documents of interest, see the Endnotes, starting on page 47.*

## II. Incident Management

### Overview

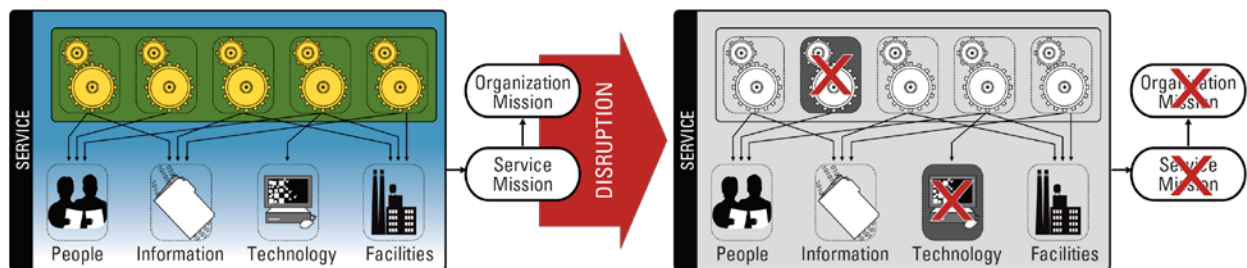


Figure 1: Disruption

Disruptions to an organization’s operations may occur regularly and can scale from so small that the impact is essentially negligible to so large that they could prevent an organization from achieving its mission (see Figure 1). The required responses to these disruptive events must scale similarly. Some events may not require a formal response by the organization and can be effectively ignored or handled at the individual level following standard operating procedures. For example, a workstation may lock up, preventing the processing of new

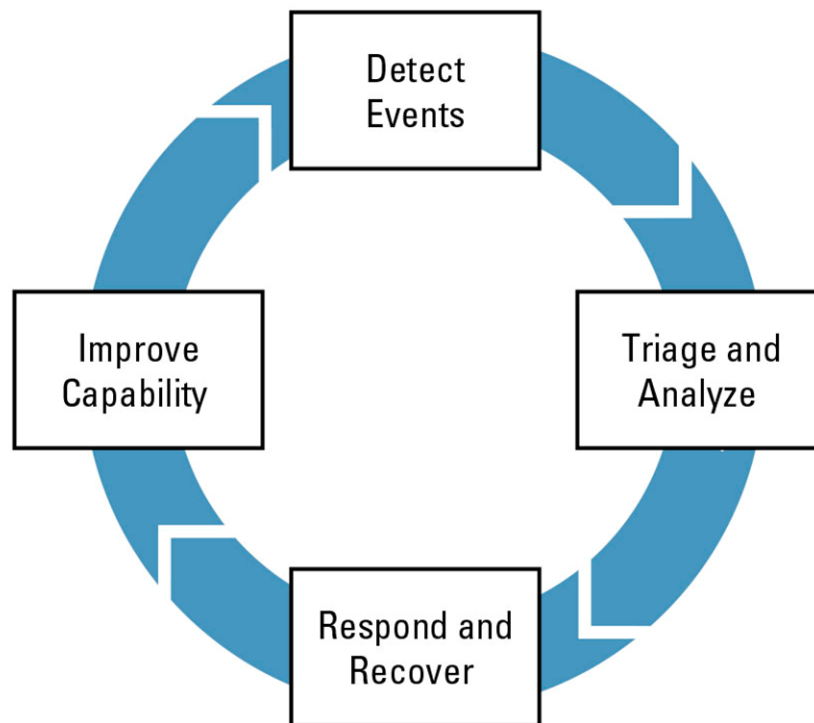


orders. Addressing this interruption may only require the individual workstation owner to perform a simple reboot. Once the workstation reboots, orders can be processed again. The event required a response, but that response was carried out by a single individual. Other disruptive events require the entire organization to mobilize resources. Examples of events whose management may require significant resource investment include natural disasters, loss of a primary data center, a cyber attack that disrupts critical organizational infrastructure, or any event that affects the organization's ability to deliver critical services.

The process of detecting, analyzing, responding to, and improving from disruptive events is known as incident management. The goal of incident management is to mitigate the impact of a disruptive event. To accomplish this goal, an organization establishes processes that

- detect and identify events
- triage and analyze events to determine whether an incident is underway
- respond and recover from an incident
- improve the organization's capabilities for responding to a future incident

Figure 2 depicts the incident management process.



*Figure 2: The Incident Management Process*

The following sections detail each of the steps in the incident management process.

## Detect Events

An *event* is one or more occurrences that affect an organization's assets and have the potential to disrupt its operations.<sup>4</sup> An effective incident management process requires that an organization monitor and identify events as they occur. Many units in an organization can perform this activity, but it is often the responsibility

of a help desk or network operations center. The optimal implementation of the event detection activities depends heavily on the organizational structure and the scope of the larger incident management process. For example, a smaller organization may not have a formal help desk or network operations center. Those organizations may assign event detection responsibilities to specific information technology staff or outsource event detection responsibilities to a third-party provider. No matter the specific implementation, all organizations should have capabilities to detect, report, log, track, collect, and store event evidence. The inability to identify events in a timely manner can significantly increase the organization's recovery costs and effort.

Important activities in event detection include

- event detection and reporting
- logging of event data in an incident database or similar mechanism
- event status tracking
- handling of event data in accordance with laws, rules, regulations, policies, etc.

## Triage and Analyze

An *incident* is a high-magnitude event or series of events that significantly affects organizational assets and requires the organization to respond in order to prevent or limit organizational impact.<sup>5</sup> Triaging event artifacts is the first step in an analysis process through which an organization recognizes that an incident is underway. In the triage process, an organization determines how to categorize an event or series of events, how to evaluate it, and whether the event reaches the threshold of a declarable incident. The threshold for when an incident has occurred, is occurring, or is imminent and requires a response is unique to each organization and depends on factors such as organizational structure, mission requirements, and laws and regulations. For example, a technical disruption with a time-to-repair that exceeds the acceptable recovery time of a critical service may be a threshold for declaring an incident.

*See Figure 4 on page 16 for examples of types of events that may be escalated and declared an incident.*

Once an organization recognizes an incident, it performs additional analysis to determine the appropriate response. Analysis helps the organization better understand the incident, identify appropriate actions to contain or prevent further impact from the incident, and recover and return to operations. Some organizations may have already planned specific responses to previously considered incidents. In other cases, organizations may need to collect input from all of the appropriate stakeholders to determine the best response. Stakeholders may include asset owners, senior leadership, technical staff, and dedicated incident response staff.

Important activities in the triage and analysis include

- event categorization
- events prioritization
- event data correlation and analysis
- incident declaration
- incident analysis and response determination

## Respond and Recover

Responding to and recovering from an incident requires an organization to take actions to prevent or contain the impact of an incident. This requires that organizational response be escalated to the stakeholders who are

best able to implement and manage the response and bring the incident to a close. The amount of resources and level of effort required for the organizational response will vary with the extent of the incident and should be informed by incident analysis. Appropriate responses can range from simply informing an asset owner of the occurrence of an incident to implementing service continuity plans that require relocating services and operations to a secondary location. Because there is a broad range of potential incidents, organizations must consider a broad range of potential responses. Each organization's unique operating environment determines the appropriate response and should be used by the organization to set incident response performance requirements. Examples of incident response performance requirements include response time frames for incident types, cost per incident, time from event detection to event closure, and time from incident declaration to stakeholder communication. Factors that influence an organization setting these requirements include organizational mission, critical success factors, risk appetite, and current competitive environment.

Important practices in the Respond and Recover step include

- incident escalation to stakeholders
- response development and implementation
- incident status communication
- incident tracking

## Improve Capability

Once an organization responds to an incident and its operations are no longer being disrupted, the organization should conduct a post-incident review to consider the performance of its response activities. Organizations can use this review to understand why an incident or series of incidents occurred and what the organization can do prevent them in the future. The review should include all those who participated in the response and recovery and the stakeholders whose assets were impacted by the incident. It should consider whether the response and recovery were as effective and efficient as they could have or should have been. From a risk management point of view, the organization can use the lessons learned from an incident to improve its protection and control strategies and to optimize them with its business continuity and disaster recovery plans. As with the other steps, the extent and effort required for the review depend on the impact of the incident and the organization's operating environment. Once the organization has completed its review, it is important that it close the incident. Closing the incident is an official declaration that no further action on the incident needs to be taken. Incident closure activities ensure that all of the stakeholders affected by the incident are notified that it has been addressed, and they should not see any further effects.

Important practices in improving the incident management capability include

- root cause analysis
- incident closure

## Develop a Plan

Having a defined process for identifying, analyzing, responding to, and learning from incidents that interrupt an organization's operations provides consistent response to cybersecurity incidents and ensures that objectives are met when handling an incident. Without a defined process, an organization's incident response might omit actions that the organization considers important. An incident management plan describes how the organization will respond to cybersecurity incidents. The objective of the plan should be translated into specific actions

assigned to individuals or groups to perform when an incident occurs. The incident management plan should address, at a minimum,

- the organization's approach to incident management
- the structure of the incident management process
- the requirements and objectives of the incident management process
- a description of how the organization will identify events, triage and analyze incidents, respond and recover from incidents, and improve its response capabilities over time
- the roles and responsibilities necessary to carry out the plan
- applicable training needs and requirements
- resources that will be required to meet plan objectives
- relevant costs and budgets associated with incident management activities<sup>6</sup>

The following sections of this guide lay out the discrete steps for developing a plan that implements the incident management process as described above:

### **Create an Incident Management Plan**

1. Obtain support for incident management planning.
2. Establish an event detection process.
3. Establish a triage and analysis process.
4. Establish an incident declaration process.
5. Establish an incident response and recovery process.
6. Establish an incident communications process.
7. Establish a post-incident analysis and improvement process.
8. Assign roles and responsibilities for incident management.

### **Test the Incident Management Plan**

1. Establish a testing process.
2. Conduct plan testing.
3. Record and report the results.

### **Improve the Incident Management Plan**

1. Identify signs that the incident management plan needs to be revised, and make indicated improvements to the plan.
2. Conduct a post-mortem review of plan activities.

*See Appendix A for an example incident management plan template.*

Organizations that already have an incident management plan can use the guidance in this implementation guide to assess and make improvements to the existing plan.



### III. Create an Incident Management Plan

#### Before You Begin

The following checklist summarizes the tasks you will need to complete and the information you will need to gather before you can begin developing an incident management plan.

	Input	Guidance
✓	Scoping statement	This statement defines what needs to be addressed by the incident management plan. The plan could be scoped to cover all organizational operations or just a single business unit or organizational service. For organizations that are not sure where to start, focusing on a critical service and the areas that directly affect its performance may allow an organization to address the areas of greatest risk first and mitigate their impact while practices are being more fully developed. If your organization has participated in a CRR, it may be beneficial to begin with the critical service addressed during the CRR. See Appendix E for a cross reference between the CRR and this guide.
✓	Lists of stakeholders	The list of stakeholders should be aligned to the scoping statement and include all appropriate internal and external entities. Potential candidates include <ul style="list-style-type: none"> <li>Internal <ul style="list-style-type: none"> <li>executive and senior management</li> <li>heads of business lines, especially critical services owners</li> <li>information technology</li> <li>legal</li> <li>board of directors</li> </ul> </li> <li>External <ul style="list-style-type: none"> <li>customers and providers who may be impacted in the event of an incident</li> <li>first responders, such as law enforcement, fire, and medical</li> <li>technology support vendors and recovery partners (i.e., disaster recovery services)</li> <li>infrastructure providers, such as data and telephony and regulatory agencies</li> </ul> </li> </ul>
✓	Management support	<ul style="list-style-type: none"> <li>An endorsement by senior management for conducting incident management planning activities and implementing processes</li> </ul>
✓	An understanding and acknowledgement of an acceptable approach to incident management planning	<ul style="list-style-type: none"> <li>Acknowledgement of the intended approach to incident management, including stakeholder expectations about acceptable response objectives; this information may be contained within contracts, participation agreements, or other service-level agreements.</li> </ul>

✓	Externally imposed requirements for incident management	<ul style="list-style-type: none"> <li>Regulatory requirements defining mandatory incident reporting requirements, and other needs</li> <li>Service-level agreement requirements</li> </ul>
✓	Assignment of responsibility for incident management	<ul style="list-style-type: none"> <li>Job descriptions and performance reviews including responsibilities for incident management, for example, executive decisions, incident management, communication, event and incident response, testing, and emergency preparedness</li> </ul>
✓	Budget for incident management planning	<ul style="list-style-type: none"> <li>Identification of available funds to perform incident management planning and execution, including <ul style="list-style-type: none"> <li>staffing resources</li> <li>tools (applications and associated hardware)</li> <li>third-party support</li> </ul> </li> </ul>

## Step 1. Obtain support for incident management planning.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
<b>Goal 1: A process for identifying, analyzing, responding to, and learning from incidents is established.</b>	—
1. Does the organization have a plan for managing incidents? [IMC:SG1.SP1]	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability. PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.
2. Is the incident management plan reviewed and updated? [IMC:SG1.SP1]	DE.DP-5: Detection processes are continuously improved. PR.IP-10: Response and recovery plans are tested.

Management support and participation is an essential requirement for an incident management plan to be effective. If no incident management plan exists in your organization, and there is no mandate from senior management to establish such a plan, it will likely be necessary to obtain executive-level approval and support for the creation of the plan. What level of management support is required entirely depends on the scope of the incident management plan. Senior-executive-level support is probably necessary for a plan that covers an entire organization. For plans that are scoped to an individual service, the only necessary sponsorship may be from senior management responsible for the service.

*A common way for organizations to demonstrate support is to create policy that requires or defines incident management activities. See Appendix B for an example cybersecurity policy template.*

## Step 2. Establish an event detection process.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
<b>Goal 2: A process for detecting, reporting, triaging, and analyzing events is established.</b>	—
1. Are events detected and reported? [IMC:SG2.SP1]	DE.CM-1: The network is monitored to detect potential cybersecurity events. DE.CM-2: The physical environment is monitored to detect potential cybersecurity events. DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events. DE.DP-4: Event detection information is communicated to appropriate parties. RS.CO-2: Events are reported consistent with established criteria.

Events must be captured and analyzed so that the organization can determine if the event will become (or has become) an incident that requires action. The extent to which an organization identifies events improves its ability to manage and control incidents and their potential effects.

**A. Establish an event detection and reporting process.**

- i. Define *event* for your organization and document the definition. For example, an event is “one or more occurrences that affect organizational assets and have the potential to disrupt operations.”<sup>7</sup> Further, an event may be any observable or measurable occurrence in the organizations’ systems or networks. Events may include, but are not limited to, a user logging into an account, a web server receiving a request for a specific web page, a user accessing files on network share, and a firewall blocking a connection attempt.
- ii. For each type of event, identify associated methods of event detection.<sup>8</sup> Event detection methods may include
  - monitoring of technical infrastructure, including network architecture and network traffic, via such tools as intrusion detection systems, packet inspection services, firewalls, and data integrity tools
  - reporting of problems or issues to the organization’s service desk<sup>9</sup>
  - monitoring of users of IT services
  - monitoring environmental and geographical events reported through the media
  - receiving reports from legal or law enforcement staff
  - observing the breakdown of processes or productivity of assets
  - receiving external notification from other entities such as US-CERT

*For further information about US-CERT, including alerts, current activity, products in the National Cyber Awareness System, tips, and bulletins, go to <http://www.us-cert.gov>.*

- reviewing the results of audits or assessments

**B. Establish an event data logging process.<sup>10</sup>**

- i. Define how event data will be captured in your organization. For each type of event data, determine how it will be logged and how those logs will be monitored. Typical activities can include
  - enabling logging on firewalls, servers, and monitoring software
  - enabling automatic alerts where possible
  - defining a schedule for manual log monitoring where automatic alerts are not possible
  - creating automatic logging notification and response rules in service or help desk and network monitoring software systems
- ii. Establish an event knowledge base or similar mechanism to facilitate event triage and analysis activities.<sup>11</sup> Data in knowledge base should include
  - unique identifier
  - brief description of the event
  - event category (denial of service, virus intrusion, physical access violation, etc.)
  - assets, services, and organizational units affected by the event
  - brief description of how the event was identified and reported and by whom, as well as other relevant details (application system, network segment, operating system, etc.)
  - individuals or teams to whom the event (or incident) was assigned
  - relevant dates
  - response actions to the event<sup>12</sup>

### Step 3. Establish a triage and analysis process.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
<b>Goal 2: A process for detecting, reporting, triaging, and analyzing events is established.</b>	—
2. Is event data logged in an incident knowledge base or similar mechanism? [IMC:SG2.SP2]	DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors.
3. Are events categorized? [IMC:SG2.SP4]	RS.AN-4: Incidents are categorized consistent with response plans.
4. Are events analyzed to determine if they are related to other events? [IMC:SG2.SP4]	DE.AE-2: Detected events are analyzed to understand attack targets and methods.

- A. Establish an event categorization process.** Categorizing means that the organization has defined categories for events, applies the categories to events, and records those categories in the event knowledge base described above.

*Figure 4 on page 16 provides examples of types of events that may become incidents depending on their categorization.*

- i. Define event categories for your organization. Events may be categorized by type (e.g., security, safety, unauthorized access, user issue, denial of service), severity (e.g., critical, high, medium, low), and other characteristics. Examples of common event categories include
  - o type of response required
  - o type of notification required
  - o escalation indicated in incident management plan<sup>13</sup>
  - o software or hardware component failure
  - o intrusion or malware<sup>14, 15</sup>
- B. Define an event analysis process to identify related events.**<sup>16</sup> Cybersecurity events should be analyzed to determine whether they are related to other events. Such a relationship may indicate that the events are symptomatic of a larger issue, problem, or incident. For example, significant unexplained increases in network traffic may indicate unauthorized activity on the source or destination devices. When an event is escalated to an incident, further analysis supports incident triage. Through triage, the organization determines the type and extent of an event, whether the event correlates to other events, and in what order events should be addressed or assigned for incident declaration, handling, and response.
  - i. Establish criteria for event comparison, for example, the output of logging software or system monitoring.
  - ii. Establish guidelines for correlating events.<sup>17, 18</sup> For example:
    - o Is the event isolated?
    - o Is the event appearing in a number of systems or locations?
    - o Does this event appear to be a symptom or cause of other events?
    - o Does this event appear to be related to potential threats discovered through vulnerability analysis or situational awareness efforts?
- C. Define an event prioritization process.**<sup>19, 20</sup> Prioritization will facilitate an optimal response, when a response is necessary. Prioritization may be informed by event knowledge base information, the results of categorization and correlation analysis, incident declaration criteria, and experience with past declared incidents. Most help desk tools can automatically prioritize events based on a rule set defined by your organization.
  - Event prioritization (e.g., high, medium, or low) should indicate the impact, time frame for response, type of response, and escalation required.
  - The highest event priority may also be extended to include criteria for incident declaration.



- D. Define an event status tracking process.**<sup>21</sup> The process should establish a predefined frequency for tracking events.<sup>22</sup> The frequency may be based on event prioritization. Examples of tracking and reporting status may include<sup>23</sup>
- event in progress with expected time to resolution
  - closed
  - referred for further analysis
  - referred to organizational unit or line of business for disposition
  - declared as incident and referred to incident handling and response process
- E. Define a process for identifying event evidence as required by law or other obligations.**<sup>24</sup>
- i. Document requirements for identifying event evidence for forensic purposes.
  - ii. Cite pertinent rules, laws, regulations, and internal policies.<sup>25, 26</sup>
- F. Define a process for handling forensic evidence.**<sup>27</sup>
- i. Create a written process for collecting and preserving forensic evidence as required by pertinent rules, laws, regulations, and internal policies.<sup>28</sup>
  - ii. Establish training requirements in accordance with rules, laws, regulations, and internal policies.<sup>29</sup>

#### Step 4. Establish an incident declaration process.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
<b>Goal 2: A process for detecting, reporting, triaging, and analyzing events is established.</b>	—
3. Are events categorized? [IMC:SG2.SP4]	RS.AN-4: Incidents are categorized consistent with response plans.
<b>Goal 3: Incidents are declared and analyzed.</b>	—
1. Are incidents declared? [IMC:SG3.SP1]	RS.CO-2: Events are reported consistent with established criteria.

- A. Establish and document predefined criteria for incident declaration for your organization.**<sup>30, 31, 32, 33</sup>

*See Appendix C for example cybersecurity incident declaration criteria.*

- i. Identify and document executives and staff who have the authority to declare an incident and assign responsibility and authority for declaring incidents.
- ii. Establish notification and communication requirements at incident declaration.
- iii. Define a declaration process that includes predefined and documented criteria for incident declaration and conditions under which declaration requires escalation. Criteria may include
  - risk to life or safety
  - scope of the event (i.e., percentage of affected technology, geographic distribution)
  - cybersecurity incident such as
    - a violation of (company/agency) computer security policies and standards
    - unauthorized computer access
    - loss of information confidentiality
    - loss of information availability
    - compromise of information integrity
    - a denial-of-service condition against data, network, or computers
    - misuse of service, systems, or information
  - physical or logical damage to systems

- potential financial impact
- risk to delivery of the critical service
- availability of key executives
- incidents that are self-evident, in that they meet declaration criteria on detection

**B. Establish a process for incident analysis to determine the appropriate response.<sup>34</sup>**

- Identify and document the method of and parties responsible for incident analysis. Steps for an incident analysis process should include the following:<sup>35</sup>
  - Establish and communicate a standardized and consistent incident analysis approach and structure.
  - Identify relevant analysis tools, techniques, and activities that the organization will use to analyze incidents and develop appropriate responses. Provide incident management staff the appropriate levels of training on analysis tools and techniques.<sup>36</sup>
  - Analyze open event reports and previously declared incidents. Open event reports may correlate to the incident under analysis and provide additional information that is useful in developing an appropriate response. Reviewing documentation on previously declared incidents may inform the development of a response action plan, particularly if significant organizational (and external) coordination is required.
  - Document analysis in an incident report.
  - Ensure that the analysis documented in the incident report is also documented in the incident knowledge base and made available for use in evidence collection, response development, and post-incident review.
- Categorize incidents based on the type of response, notification, and escalation indicated in the incident management plan. Categories may include
  - information security
  - facilities
  - physical security
  - staff safety
  - pandemic
  - public relations

**Step 5. Establish an incident response and recovery process.<sup>37</sup>**

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
<b>Goal 4: A process for responding to and recovering from incidents is established.</b>	—
1. Are incidents escalated to stakeholders for input and resolution? [IMC:SG4.SP1]	RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams. RS.CO-4: Coordination with stakeholders occurs consistent with response plans.
2. Are responses to declared incidents developed and implemented according to predefined procedures? [IMC:SG4.SP2]	RS.MI-1: Incidents are contained. RS.RP-1: Response plan is executed during or after an event.
3. Are incident status and response communicated to affected parties? [IMC:SG4.SP3]	RC.CO-1: Public Relations are managed. RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams. RS.CO-3: Information is shared consistent with response plans.
4. Are incidents tracked to resolution? [IMC:SG4.SP4]	RS.MI-1: Incidents are contained. RS.MI-2: Incidents are mitigated.

Some organizations establish one or more permanent teams with the repeatable capability to respond to a broad range of incidents. In other cases, an organization may establish a virtual team of individuals who may be quickly called on to perform specific incident response duties.<sup>38</sup> Figure 3 shows an example of standing and virtual response teams.

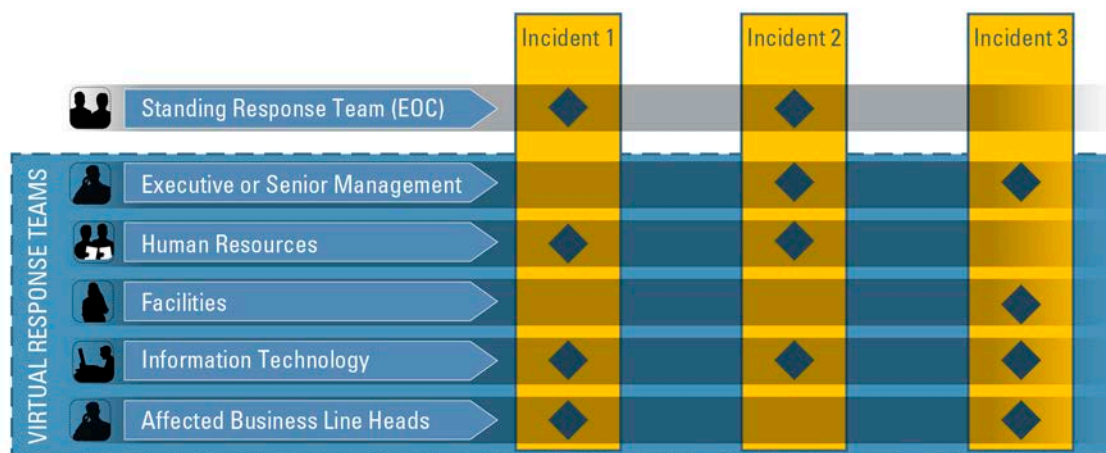


Figure 3: Response Team Example

**A. Escalate incidents to stakeholders.** Stakeholders should be predefined and include those staff required to assist in incident analysis, triage, and response; those potentially impacted by the incident; and staff responsible for coordination and status communication.

- i. Identify stakeholders for each category of incident.<sup>39</sup>
- ii. Establish a format for event status reporting.

*See Appendix D for an example reporting template.<sup>40</sup>*

- iii. Communicate incident status and response to affected parties.

**B. Develop and implement responses to declared incidents.**

- i. Develop predefined procedures for each category of incident. Predefined procedures should include<sup>41</sup>
  - o internal and external communications plans<sup>42</sup>
  - o service continuity plans
    - IT disaster recovery
    - business continuity
  - o medical response and pandemic plans
  - o first responder plans, such as police and fire
- ii. Develop an incident management report format to be used by the Incident Manager.

*See Appendix D for an example incident reporting template.*

- iii. Develop procedures for your incident management team to follow once the team is assembled. If your organization does not have an Emergency Operations Center (EOC) with prescribed procedures, you will need to establish procedures for the incident management team. The team is formed from the previously identified stakeholders, as defined in the incident management plan. Response procedures should include

- essential activities that are required to contain or limit damage and ensure the continuity of the critical service
- resources and skills required to perform the incident response plan
- coordination activities with other internal staff and external organizations to implement the strategy
- activities essential to restoring services to normal operation (recovery), the resources involved in these activities, and their estimated cost
- legal and regulatory obligations that the strategy must meet

**C. Track incidents to resolution.**<sup>43</sup>

- i. Establish a predefined frequency for tracking incident status. The frequency may be based on a predetermined schedule. Examples of tracking and reporting statuses may include
  - incident in progress with expected time to resolution
  - closed
  - incident knowledge base updated<sup>44</sup>

**Step 6. Establish an incident communications process.**

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
<b>Goal 4: A process for responding to and recovering from incidents is established.</b>	—
1. Are incidents escalated to stakeholders for input and resolution? [IMC:SG4.SP1]	RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams. RS.CO-4: Coordination with stakeholders occurs consistent with response plans.
3. Are incident status and response communicated to affected parties? [IMC:SG4.SP3]	RC.CO-1: Public Relations are managed. RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams. RS.CO-3: Information is shared consistent with response plans.

Communication is an important function of incident management. Organizations must have a flexible and quickly activated incident communications capability throughout the incident management process, including event detection, incident escalation, triage, analysis, response, and recovery. Initial information may be inaccurate and incomplete, causing confusion. As the situation becomes clearer and events escalate to incidents, the focus tends to be on mitigating the impact of the incident rather than continued communications to stakeholders.<sup>45</sup> Coordination and communication are essential throughout. Figure 4 provides an example of multiple event paths escalated through the incident management process, in which communication to affected stakeholders is required.

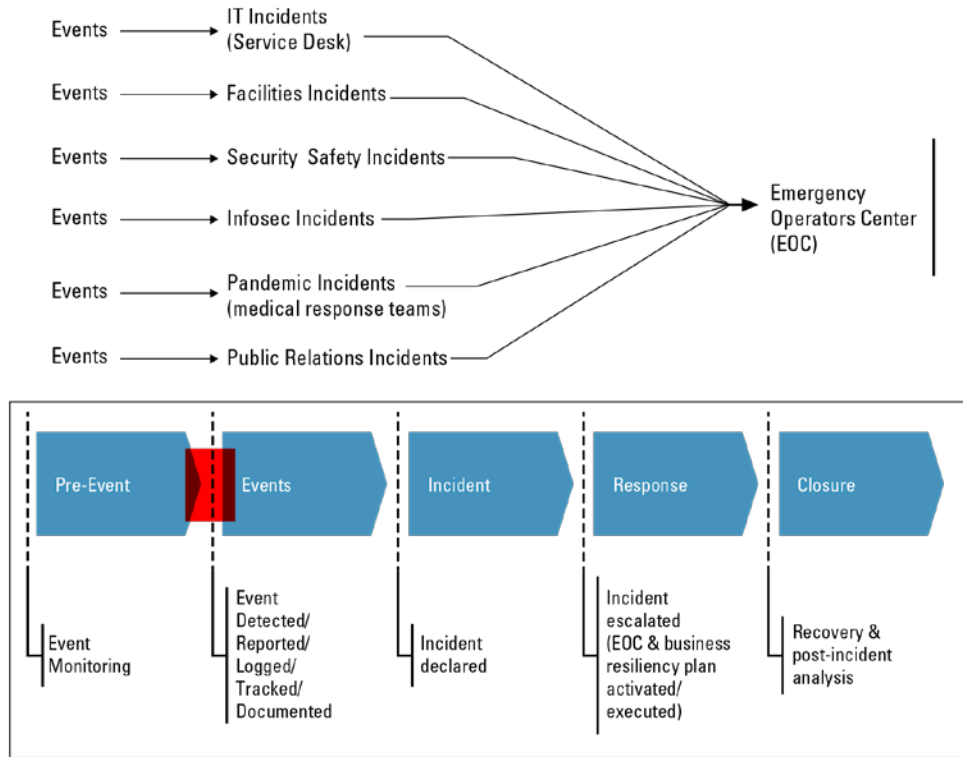


Figure 4: Example Event and Incident Escalation Path

**A. Identify primary contacts.**

- Identify groups or teams, and the individuals they comprise, who must be contacted in each step of the incident management and control process.
- Create contact lists for each group or team. Contact lists should contain, at a minimum, staff names, roles, locations (office, home, or second home), and communication device such as office, pager, cellular phone, home, and email. Figure 5 provides a sample template for team contact information.

Incident Management Team Contact Information					
Name	Office	Pager	Cell	Home	Email

Alternate Member Information					
Name	Office	Pager	Cell	Home	Email

Figure 5: Example Team Contact Information Template

**B. Identify backup contacts.**

- i. Identify an alternate for every primary contact; record the alternate's contact information.
- ii. Establish a protocol for contacting backups. For example, if primary contacts do not respond in 1 hour from initial incident notification, start sending incident notifications to backup contacts.

**C. Establish a communications plan;** ensure that it addresses methods and infrastructure.

- i. Leverage any existing communications plan, infrastructure, and staff. However, it may be necessary to add protocols, contact groups, and emergency-focused responsibilities. Additions and modifications should be made as part of the incident management plan, and capabilities should be integrated into plan execution.<sup>46, 47</sup> If no communications plan exists, create an incident communications plan with roles and responsibilities for each aspect of communication, including
  - external organization communication, including media
  - organization-wide communication
  - contact list initiation
- ii. Establish an EOC. Many organizations have an EOC as a physical command center from which to conduct emergency operations. If your organization does not have an EOC, it may be necessary to convene the incident management team virtually using a bridge line or conferencing capabilities.
- iii. Establish virtual meeting capability, including
  - conference or bridge lines with sufficient capacity to accommodate individual or multiple teams as necessary
  - a communication method, such as call lists or use of an automated speed dialing system
  - secure access

- protocols for meetings, such as meeting leadership and emergency management checklists
- protocols for recording and reporting status
- iv. Establish alternate physical meeting locations and include protocols for use.<sup>48</sup>

## Step 7. Establish a post-incident analysis and improvement process.<sup>49</sup>

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
<b>Goal 5: Post-incident lessons learned are translated into improvement strategies.</b>	—
1. Is analysis performed to determine the root causes of incidents? [IMC:SG5.SP1]	DE.DP-5: Detection processes are continuously improved. PR.IP-7: Protection processes are continuously improved.
2. Is there a link between the incident management process and other related processes (problem management, risk management, change management, etc.)? [IMC:SG5.SP2]	DE.DP-5: Detection processes are continuously improved. PR.IP-7: Protection processes are continuously improved.
3. Are lessons learned from incident management used to improve asset protection and service continuity strategies? [IMC:SG5.SP3]	DE.DP-5: Detection processes are continuously improved. PR.IP-7: Protection processes are continuously improved. RS.IM-1: Response plans incorporate lessons learned. RS.IM-2: Response strategies are updated.

The post-incident and analysis process is essential in identifying areas that need improvement. The incident may have exposed flaws in the incident management process, which can be further investigated under controlled testing conditions. Convene a team of stakeholders involved in the incident. Stakeholders may change based upon the type of incident. Figure 6 shows how different event streams flow through the incident management process, from which stakeholders may be selected. Conduct a tabletop walkthrough of the incident process, reviewing actions taken and status reports. If possible, determine the root cause of the incident, which may include failure of internal processes. Identify what went well and areas for improvement.

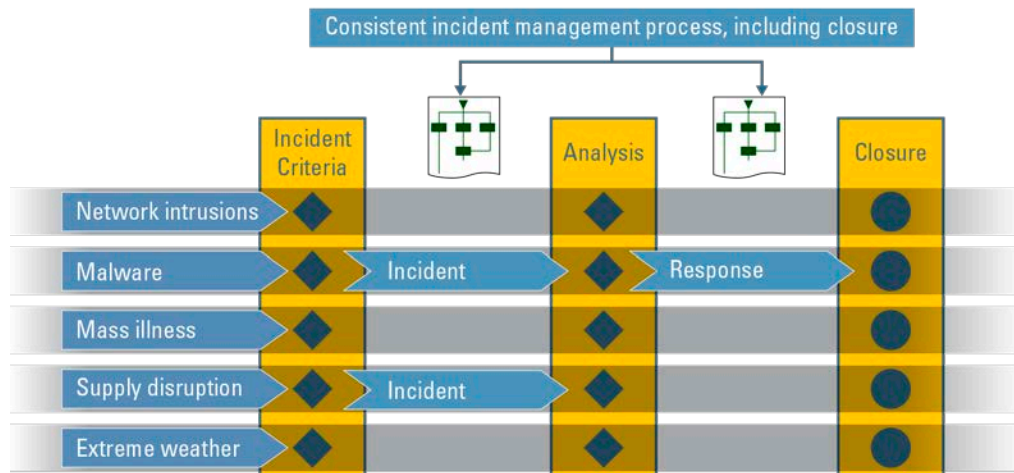


Figure 6: Incident Management and Control Process Example

### A. Analyze the incident to determine root causes.

- i. Establish a team to perform post-incident analysis.
- ii. Document analysis procedures.<sup>50</sup>
- iii. Establish a schedule for the post-incident analysis.

### B. Identify links between the incident management process and other processes, and determine if links performed as required.<sup>51, 52</sup> Areas often related to incident management are



- communications
- risk management
- monitoring
- service continuity

**C. Use lessons learned from the incident to improve asset protection and service continuity strategies.**<sup>53</sup>

Areas that could benefit from lessons learned include

- protection strategies and controls for assets involved in the incident
- continuity plans and strategies for sustaining assets involved in the incident<sup>54</sup>
- information security and other organizational policies that need to reflect new standards, procedures, and guidelines based on lessons learned<sup>55</sup>
- staff training on information security, business continuity, and IT operations

## Step 8. Assign roles and responsibilities for incident management.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
<b>Goal 1: A process for identifying, analyzing, responding to, and learning from incidents is established.</b>	—
3. Are the roles and responsibilities in the plan included in job descriptions? [IMC:SG1.SP2]	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability. PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening).
4. Have staff been assigned to the roles and responsibilities detailed in the incident management plan? [IMC:SG1.SP2]	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability. RS.CO-1: Personnel know their roles and order of operations when a response is needed.

Identify roles that will be filled from within your organization and those that must be filled externally. Table 1 provides an example of incident management responsibilities assigned to specific organizational roles. Incident management roles may vary based on the structure and capabilities of your organization.<sup>56, 57</sup> For example, you may be able to support functions such as communication, event detection, incident declaration, information technology and business recovery, and status reporting but have to identify external dependencies for physical security, fire, health and safety, and electrical power.<sup>58</sup> Identify the area within your organization that will interface with each outside entity.

**A. Identify the areas in your organization that are best suited to support each of the functional components of the plan, and identify roles that must be filled in each area to perform plan tasks.**<sup>59</sup>

**B. Assign staff by name to incident management plan functions and tasks.** Formalize roles and responsibilities. Add incident management duties to job descriptions, and include the performance of those duties in performance reviews.<sup>60</sup> An incident management plan will typically have the roles and responsibilities shown in Table 1, though they may vary by organization.

*Table 1: Incident Management Roles and Responsibilities*

Role	Responsibility
Executive Management	A senior executive is usually designated as the sponsor for the incident management program and serves as the immediate escalation point for critical decisions.
Incident Management	An Incident Manager (or managers, depending on the duration of the incident) usually directs incident management activities, informs executive management, and escalates the incident as necessary. The Incident Manager directs incident status meetings and reporting.



Role	Responsibility
Communications	<p>The importance of communications is typically underrated in incident management. Communications may be a stand-alone function or may reside within another area such as Technology. Responsibilities include establishing and executing a communications plan with procedures and protocols for both internal and external communication as well as the supporting equipment and infrastructure. Example duties include the following:</p> <ul style="list-style-type: none"> <li>• Coordinate all media communications.</li> <li>• Review and approve all statements regarding the incident.</li> <li>• Develop both internal and external communications.</li> <li>• Coordinate recovery-related advertising with external vendors.</li> </ul>
Human Resources	<p>Human Resources is usually responsible for the well-being of employees. This includes providing information about medical coverage, pandemic or personnel loss planning, succession planning, family and casualty support, and sometimes personal safety. Example duties include the following:</p> <ul style="list-style-type: none"> <li>• Account for all personnel.</li> <li>• Ensure the health and safety of employees.</li> <li>• Coordinate employee communications with Communications.</li> <li>• Coordinate additional or temporary staffing for recovery effort.</li> </ul>
Technology	<p>Technology usually refers to information technology, but it may include manufacturing or other types of equipment that are not the responsibility of Facilities. Technology is primarily responsible for IT disaster recovery, as part of service continuity planning. Technology is usually responsible for cybersecurity and maintaining related contacts with law enforcement. Example duties include the following:</p> <ul style="list-style-type: none"> <li>• Conduct computer system and telecommunications damage assessment.</li> <li>• Activate alternate operating locations (for system recovery).</li> <li>• Recover computer systems and network environment(s).</li> <li>• Ensure all system security devices and procedures are in place.</li> </ul>
Heads of Business Lines	<p>Critical services or business lines are usually represented by the senior manager responsible for the service, as well as support staff.</p>
Legal	<p>The senior attorney and, often, risk managers advise the response team on matters involving liability, compliance, records management, and regulatory requirements. Example duties include the following:</p> <ul style="list-style-type: none"> <li>• Manage all required regulatory notifications.</li> <li>• Provide legal counsel for response and recovery operations.</li> <li>• Review and approve new contracts acquired as a result of the event, before the contracts are implemented.</li> </ul>
Insurance	<p>A representative responsible for insurance matters advises the team when matters of indemnification are involved. Example duties include the following:</p> <ul style="list-style-type: none"> <li>• Coordinate with an insurance broker on the preparation and filing of all insurance claims.</li> <li>• Document proof of losses.</li> <li>• Submit claims and monitor payments.</li> </ul>
Facilities	<p>Facilities is usually responsible for safety, evacuation, hazards, and fire response. Example duties include the following:</p> <ul style="list-style-type: none"> <li>• Conduct a detailed damage assessment.</li> <li>• Ensure that response activities to address fire, spills, and/or medical emergencies are performed in accordance with policies and guidelines.</li> <li>• Enlist the assistance of vendors and agencies in support activities as appropriate.</li> <li>• Conduct salvage and restoration activities.</li> </ul>
Physical Security	<p>Security typically refers to physical security and is the primary contact for law enforcement and emergency medical response. Example duties include the following:</p> <ul style="list-style-type: none"> <li>• Coordinate on-site security for affected facilities and all alternate operating locations.</li> <li>• Control access to affected facilities.</li> <li>• Monitor equipment and records being removed from facilities.</li> </ul>

Role	Responsibility
Finance	<p>Finance is typically responsible for emergency funding for procurement, purchasing, travel, lodging, and other response requirements. Example duties include the following:</p> <ul style="list-style-type: none"> <li>• Ensure funds are available for recovery.</li> <li>• Set up a recovery cost center.</li> <li>• Estimate the impact of the incident on the company's financial statement.</li> <li>• Manage all incident-related purchasing.</li> </ul>

## Output of Section III

	Output	Guidance
✓	Enterprise guidance for incident management	Organization-wide standards for managing incidents
✓	Executive endorsement and participation in incident management planning and incident response	Visible support from executive management for incident management activities; executive leadership during an incident, as required
✓	Identified stakeholders for incident management	All participants in the incident management process will be assigned and be aware of their roles and responsibilities.
✓	Identified laws, regulations, and rules	List of requirements for the organization when operating during a disaster or disruption
✓	Statement of incident management strategy	A written description of how incident management operations should be conducted throughout the organization, ensuring that all response efforts are consistent
✓	Detailed processes for incident management	<p>Predefined processes for detecting, reporting, communicating, analyzing, and responding to incidents, including providing</p> <ul style="list-style-type: none"> <li>• an incident communications process</li> <li>• an incident declaration and analysis process</li> <li>• an incident response and recovery process</li> <li>• a post-incident analysis and improvement process</li> </ul>

Once your organization has documented its incident management plan, standards, and guidelines, it should periodically review and update them, at least annually or as required by regulation or other guidelines, to ensure that they are achieving the desired results.



## IV. Test the Incident Management Plan

By testing your incident management plan, you allow your organization and the personnel directly involved in managing incidents the opportunity to practice roles and responsibilities in a controlled environment. You also ensure that the plan produces the desired outcomes when tested. Incident management exercises are not meant to result in pass/fail “grades.” Instead, they should be viewed as opportunities to measure plan performance and to expose any unexpected outcomes, conflicts, and needed improvements in a controlled environment.

### Before You Begin

The following checklist summarizes the tasks you will need to complete and the information you will need to gather before you can begin testing incident management plans.

	Input	Guidance
✓	Obtain approval from stakeholders to test	<ul style="list-style-type: none"> <li>Establish the scope of testing to be conducted</li> <li>Establish the schedule of testing to be conducted</li> </ul>

### Step 1. Establish a testing process.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
<b>Goal 1: A process for identifying, analyzing, responding to, and learning from incidents is established.</b>	—
1. Does the organization have a plan for managing incidents? [IMC:SG1.SP1]	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability. PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.
2. Is the incident management plan reviewed and updated? [IMC:SG1.SP1]	DE.DP-5: Detection processes are continuously improved. PR.IP-10: Response and recovery plans are tested.

There are many approaches to testing, and the testing process may be progressive. Organizations typically begin with plan reviews, proceed to tabletop walkthroughs, and finally conduct partial to full plan tests. Contact lists can be exercised from the beginning, and such exercises should include alternate contacts and sometimes occur unannounced and during off hours.

- A. If your organization has a process for testing service continuity plans, the testing criteria and schedule may be modified to accommodate the incident management plan.**
- B. If no testing process exists, create a process, including testing criteria and a testing schedule for the incident management plan.** The process should address scope, types of tests, what to test, scenario creation, objectives, and testing frequency.

## Step 2. Test the incident management plan.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
<b>Goal 5: Post-incident lessons learned are translated into improvement strategies.</b>	—
3. Are lessons learned from incident management used to improve asset protection and service continuity strategies? [IMC:SG5.SP3]	DE.DP-5: Detection processes are continuously improved.
	PR.IP-7: Protection processes are continuously improved.
	RS.IM-1: Response plans incorporate lessons learned.
	RS.IM-2: Response strategies are updated.

It is usually best to begin by testing components of the plan rather than the plan as a whole. A component to test first—and often—is the notification and convening of the incident management team.

### A. Select an incident management plan component to test.<sup>61</sup>

- Examples include emergency communications and escalation, incident streams, and partial to full plan scenarios. Incident streams may include information technology, facilities, security and safety, information security, pandemic, and public relations impacts.
- Testing should progress in stages, such as
  - a. plan review
  - b. tabletop test or walkthrough<sup>62</sup>
  - c. component testing, such as incident declaration and team notification
  - d. limited scenario testing, using an isolated incident or a single-category incident as in an IT failure
  - e. large-scale incident testing, using a regional disaster or pandemic and testing cross-plan dependencies

**B. Create a scenario for the type of test selected.** The scenario should be scripted and include a reasonable scope and objectives, participants, and time frame.

**C. Schedule and execute the test.** Participants should be available for the duration of the test. Some component testing, such as response team notification, should be tested outside of normal working hours.

## Step 3. Record and report the results.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
<b>Goal 2: A process for detecting, reporting, triaging, and analyzing events is established.</b>	—
2. Is event data logged in an incident knowledge base or similar mechanism? [IMC:SG2.SP2]	DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors.
<b>Goal 5: Post-incident lessons learned are translated into improvement strategies.</b>	—
3. Are lessons learned from incident management used to improve asset protection and service continuity strategies? [IMC:SG5.SP3]	DE.DP-5: Detection processes are continuously improved.
	PR.IP-7: Protection processes are continuously improved.
	RS.IM-1: Response plans incorporate lessons learned.
	RS.IM-2: Response strategies are updated.

By documenting your organization's plan and standards for testing, you ensure that plan exercises can produce verifiable evidence of your capability to respond to incidents.

**A. Retain test records to gauge performance against objectives over time and identify corrective action.**

**B. Establish a reporting schedule to keep management informed of progress.**

## Output of Section IV

	Output	Guidance
✓	Guidelines and standards for incident management plan exercises	<ul style="list-style-type: none"> <li>• Identification and responsibilities of plan owners</li> <li>• Identification and involvement of stakeholders</li> <li>• Exercise management</li> <li>• Plan exercise schedule</li> <li>• Requirements for what information must be documented during and after a plan exercise</li> <li>• Measures for how the organization evaluates incident management plan performance</li> </ul>
✓	Exercise plans	<ul style="list-style-type: none"> <li>• A plan developed using pre-established exercise criteria</li> </ul>
✓	Plan exercise results	<ul style="list-style-type: none"> <li>• Acceptable response times and process adherence in accordance with the plan</li> </ul>
✓	Strategy for testing and maintaining the incident management plans	Guidelines for plan testing; using lessons learned to improve the incident management plan



## V. Improve the Incident Management Plan

Changes in the operating environment, including staff changes, evolving relationships with business associates, and newly identified risks, may require your organization to modify its incident management plan. Testing or executing your organization's continuity plans might also reveal needed updates. Because operating environments may change frequently, your organization should establish criteria for changes and manage changes to the plans through regular reviews, updates, and version control.

### Before You Begin

The following checklist summarizes the tasks you will need to complete and the information you will need to gather before you can begin improving incident management plans.

	Input	Guidance
✓	Change criteria for continuity plans	<ul style="list-style-type: none"> <li>The incident management plan must be reviewed during any major change to the organization and after the plan has been tested.</li> <li>Post-incident analysis results indicate needed improvements to the plan.</li> </ul>

### Step 1. Identify signs that the incident management plan needs to be revised, and make indicated improvements to the plan.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
<b>Goal 1: A process for identifying, analyzing, responding to, and learning from incidents is established.</b>	—
2. Is the incident management plan reviewed and updated? [IMC:SG1.SP1]	DE.DP-5: Detection processes are continuously improved. PR.IP-10: Response and recovery plans are tested.
<b>Goal 5: Post-incident lessons learned are translated into improvement strategies.</b>	—
3. Are lessons learned from incident management used to improve asset protection and service continuity strategies? [IMC:SG5.SP3]	DE.DP-5: Detection processes are continuously improved. PR.IP-7: Protection processes are continuously improved. RS.IM-1: Response plans incorporate lessons learned. RS.IM-2: Response strategies are updated.

To maintain the viability of your organization's incident management plan, identify and understand the organizational and operational triggers that may indicate a need to the plan. Once the change criteria have been met, the following steps will aid in making improvements.

**A. Review the post-incident analysis or test results with stakeholders.**

**B. Assess performance against objectives.**

**C. Determine areas for improvement.**<sup>63</sup>

- D. Establish objectives for improvement.**
- E. Schedule and implement plan improvements.**
- F. Amend the incident management plan as indicated.**<sup>64</sup>
- G. Track open items to closure.**

## Step 2. Conduct an after-action review of plan activities.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory
<b>Goal 5: Post-incident lessons learned are translated into improvement strategies.</b>	—
3. Are lessons learned from incident management used to improve asset protection and service continuity strategies? [IMC:SG5.SP3]	DE.DP-5: Detection processes are continuously improved.
	PR.IP-7: Protection processes are continuously improved.
	RS.IM-1: Response plans incorporate lessons learned.
	RS.IM-2: Response strategies are updated.

Once an incident has been closed, a review of the incident and actions taken compared to the incident management plan will reveal strengths and areas for improvement. Review the root-cause analysis at the closure of the incident. Compare actions taken to predefined procedures and identify where procedures were effective and how well they were followed.

The following are examples of activities in a typical after-action review.

### A. List all participants in the review and their role in incident management.

### B. Identify lessons learned.

- i. Describe the incident.
- ii. Discuss response and recovery, for example:
  - incident management team response
    - time to convene the team
    - initial assessment
    - leadership decisions and immediate actions taken
  - safety of employees
    - evacuation procedures and relocation
    - injuries and response
  - HR support
  - communication, both internal and external
  - IT response and recovery, including the ability to meet recovery time objectives (RTOs)
  - business operations response and recovery, including the ability to meet RTOs
  - facilities response
  - performance of external dependencies

### C. Identify what went well. Review the areas where performance met planned expectations and identify strengths.

### D. Identify areas for improvement. Identify areas where performance did not meet expectations and identify the cause.

- E. Identify corrective actions.** Assign responsibility for making improvements, including a time frame and next steps.
- F. Track open items to closure.**

## Output of Section V

	Output	Guidance
✓	Lessons learned and improvements to the incident management plan	<ul style="list-style-type: none"><li>• Lessons learned</li><li>• Strengths and weaknesses identified</li><li>• Improvements to be made</li><li>• Plan exercise schedule</li><li>• Responsibility and time frame for improvements</li></ul>





## VI. Conclusion

Establishing and supporting an ongoing incident management program enables your organization to evaluate the impact of significant events that may adversely affect employees, assets, or customers. The incident management program helps to ensure that your organization can recover its mission-critical functions and meet its responsibility to its stakeholders and its contribution to national critical infrastructure.

The following documents provide broad program guidance:

- *NIST Special Publication SP 800-61* (<http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf>) provides guidelines for handling incidents and developing a computer security response capability.
- The National Incident Management System (NIMS) (<http://www.fema.gov/national-incident-management-system>) identifies concepts and principles that address emergency management.
- The *CERT Resilience Management Model (CERT-RMM)* [Caralli 2010] is the basis for the CRR and contains more in-depth guidance for establishing practices.
- *Jane's Crisis Communication Handbook* [Fernandez and Merzer 2004] is an overall guide for establishing an incident communication program.

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

## Appendix A. Example Incident Management Plan Template

# <Organization Name> Incident Management Plan

Date: \_\_\_\_\_ Name of person completing this form: \_\_\_\_\_

## Executive Support

*List the executives who had input to this document and endorse its development and applicability.*

Name of executive	Date	Signature
<i>Sponsor</i>		
<i>Incident Manager</i>		

### Process Description

*Explain the incident management process in a manner that provides a high-level understanding to personnel who must implement this plan.*

## Critical Services

*Indicate the priority of critical services.*

Priority level	Service restoration time objective

### Plan Activation Criteria

*Describe conditions that must be met before the incident management plan can be executed.*

**Assignment of Responsibility**

List employees at your organization who are responsible for developing and maintaining this plan.

Name of employee	Date	Signature	Responsibility

**Communication Channels**

Identify communication channels to be used to notify stakeholders if this plan is to be executed.


**Key Contacts**

List the key contact information essential to the service and this plan. Include the service owner as well as internal and external technical support (examples embedded).

Name	Role	Company name	Phone 1	Phone 2
	Service owner			
	Internal technical support for information assets			
	Internal technical support for technology assets			
	External support for information assets			
	External technical support for technology assets			
	Hardware vendor			
	Primary software vendor			
	Fire company			
	Police			
	Alternate processing site contact			
	Electric utility POC			
	Telecommunications POC			
	Water utility POC			
	Executive management			
	Legal counsel			
	Internal resource for continuity plan execution			
	Internal resource for continuity plan execution			
	Internal resource for continuity plan execution			
	Stakeholder who requires notification of plan activation			

	Stakeholder who requires notification of plan activation			
	Stakeholder who requires notification of plan activation			
	Regulatory organizations that require notification if this plan is activated			
	Health-care providers who should be notified if this plan is activated			
	Other organizations that should be notified if this plan is activated			

#### **Service Owner(s)**

List the business owner(s) responsible for critical services.

<b>Name of employee</b>	<b>Date</b>	<b>Signature</b>	<b>Role</b>

#### **Essential Roles and Alternates**

Identify roles essential for incident management, as well as primary and backup/alternate personnel to perform those roles.

<b>Role</b>	<b>Primary personnel</b>	<b>Alternate personnel</b>

#### **Essential Information Assets**

List the information assets essential to incident management.

<b>Information asset name</b>	<b>Description</b>	<b>Logical location</b>	<b>Physical location</b>	<b>Backup strategy and schedule</b>

### **Special Considerations for Information Assets**

*Identify any special considerations for handling information assets in the event of plan activation.*

[illegible]

### Essential Technology Assets

*List the technology assets essential to incident management.*

[illegible]

**Primary and Alternate Site(s)**

*Identify the location(s) for command, control, and communication.*

Site name	Physical location

## Incident Management Checklist

*List the steps to follow when obtaining an incident status (examples embedded).*

Issue	Responsible party	Guidance	Status
Safety	Security, HR, Facilities		
Physical damage			
Business impact			
Immediate actions			
Media attention			

### **Plans of Action**

*List the predetermined plans and procedures to be relied on during an incident (examples embedded).*

<b>Fire and evacuation</b>	Instruct personnel to evacuate the immediate area. Locate available fire extinguishers if possible and contact fire department.
<b>Communications/media</b>	
<b>Health and safety</b>	
<b>Disaster recovery</b>	
<b>Service continuity</b>	
<b>Cybersecurity</b>	
<b>Physical security</b>	
<b>Pandemic</b>	
<b>Emergency procurement and transportation</b>	

**Schedule for testing this plan**  
**This plan will be tested <at a defined frequency>**  
**Date of last test <YYYY/MM/DD>**

*Identify any support plans that are related to this plan.*

<b>Plan name</b>	<b>Relationship</b>

## Appendix B. Example Cybersecurity Policy Template

### ***[Organization Name]* Information Technology Policy Template**

#### **POLICY [XX-X]: CYBERSECURITY INCIDENT RESPONSE**

An incident, as defined in National Institute of Standards and Technology (NIST) Special Publication 800-61, is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. An incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services.

##### **OBJECTIVE:**

Ensure that *[Organization Name]* is prepared to respond to cybersecurity incidents, to protect State systems and data, and prevent disruption of government services by providing the required controls for incident handling, reporting, and monitoring, as well as incident response training, testing, and assistance.

##### **SCOPE:**

This policy applies to all Executive Branch agencies, boards, and commissions, except those exempt under *[other policy or regulatory authority]*.

##### **RESPONSIBILITIES:**

###### **Individual Information Technology User**

All users of State or *[Organization Name]* computing resources shall be aware of what constitutes a cybersecurity incident and shall understand incident reporting procedures.

###### ***[Organization Name / CYBER Department]***

*[Organization Name / CYBER Department]* provides incident response support resources that offer advice and assistance with the handling and reporting of security incidents for users of *[Organization Name]* information systems. Incident response support resources may include *[organization-specific resources]*.

Establish a *[Cybersecurity Incident Response Team (CSIRT) or equivalent]* to ensure appropriate response to cybersecurity incidents. The *[CSIRT or equivalent]* shall consist of members of the *[Organization Name]* IT Security Council and key personnel from other agencies as required. *[CSIRT or equivalent]* responsibilities shall be defined in the *Cybersecurity Incident Reporting Procedures*.

###### **Agency Management, Information Technology Organization**

Organizations that support State information systems shall

- develop incident response plans and/or procedures that
  - provide the organization with a roadmap for implementing its incident response capability
  - describe the structure and organization of the incident response capability
  - provide a high-level approach for how the incident response capability fits into the overall organization
  - meet the unique requirements of the organization, which relate to mission, size, structure, and functions
  - define reportable incidents
  - provide metrics for measuring the incident response capability within the organization
  - define the resources and management support needed to effectively maintain and mature an incident response capability

- are reviewed and approved by designated officials within the organization
- review incident response plans and procedures at least annually
- revise the incident response plan/procedures to address system/organizational changes or problems encountered during implementation, execution, or testing
- distribute copies of the incident response plan/procedures to incident response personnel
- communicate incident response plan/procedure changes to incident response personnel and other organizational elements as needed
- when required by information system changes and annually thereafter, provide incident response training to information system users consistent with their assigned roles and responsibilities before authorizing access to the information system or performing assigned duties
- test the incident response capability of the information systems they support at least annually
  - Use organization-defined tests and/or exercises to determine incident response effectiveness. Document the results.
- implement an incident handling capability for cybersecurity incidents that includes preparation, detection and analysis, containment, eradication, and recovery
- coordinate incident handling activities with contingency planning activities
- incorporate the lessons learned from prior and ongoing incident handling activities into incident response procedures, training, and testing/exercises
- track and document information system security incidents; retain and safeguard cybersecurity incident documentation as evidence for investigations, corrective actions, potential disciplinary actions, and/or prosecutions
- promptly report cybersecurity incident information to appropriate authorities in accordance with State or organizational incident reporting procedures
- provide 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
  - Possible implementations of incident response support resources in an organization include a help desk or an assistance group and, when required, access to forensics services.

#### Document History

Version	Release Date	Comments



## Appendix C. Example Incident Declaration Criteria

### Incident Declaration Criteria

Cybersecurity incidents are to be declared and qualified as high, medium, or low when they meet the following criteria. Incidents are to be declared based on an assessment of the gravity of the situation, criticality of the service impacted, sensitivity of information threatened or compromised, and potential for harm to this organization.<sup>65</sup>

Outlined below are potential specific criteria for each of the classes (High, Medium, and Low) of cybersecurity events. This list is not all-inclusive and should be tailored to your operating environment.

#### 1. HIGH-LEVEL CYBERSECURITY INCIDENTS

High-level cybersecurity incidents are disruptions that are the most serious and are considered significant. Because of the gravity of the situation and the high potential for harm to the organization, these incidents should be handled immediately. Incidents that should be classified as “High” include events, activities, and violations such as possibly life-threatening activity, compromise of critical systems or information, root compromise, child pornography, pornographic trafficking, unauthorized music/software trafficking, and any violation of law or statute.

Incidents classified as “High” include

- suspected computer or network break-in
- website defacements or compromises, including failure to take the website offline or deregister the URL when the website is no longer used or supported by the organization
- successful denial-of-service (DoS) attacks by the organization’s cyber resources or against the organization’s cyber resources
- computer virus/worms/Trojan horses for which anti-virus software updates are not available or their deployment will be delayed
- detection of malware, including viruses, worms, Trojan horses, or spyware caused by employees who have declined to bring laptops into the office for upgrades
- connection of nonorganizational computers and servers to the organization’s network without authorization or in violation of security policies
- unauthorized use of a system for processing or storing nonorganizational or prohibited data or information on organizational cyber resources, including the establishment and operation of a private or personal business
- changes to system hardware, firmware, or software without the system owner’s authorization
- property destruction related to a cybersecurity incident (exceeding \$100,000)
- personal theft related to a cybersecurity incident (exceeding \$100,000)
- electronic file transfer (EFT) exploitation/manipulation or engaging in phishing or pharming
- installation, use, or sharing of peer-to-peer software
- activity including unauthorized or illegal serving out, downloading, or sale of copyrighted material
- child pornography
- pornography
- online gambling

- attempts to circumvent access to any organizational blocked websites such as pornography, gambling, and hate crimes
- download, use, or sharing of copyright-protected music or unauthorized software
- misuse of organizational property, facilities, or services, including accepting payment or services to provide access to or use of organizational cyber resources in excess of one's authority
- any violation of the law

## **2. MEDIUM-LEVEL CYBERSECURITY INCIDENTS**

Medium-level cybersecurity incidents are potentially serious and should be handled the same day that the incident occurs or that notification of the incident is given.

Incidents classified as "Medium" include

- adverse action resulting in employee termination in which the organization's cyber resources are neither the tool or target of the action
- Intrusion Detection System (IDS) reports that define activity as medium
- unauthorized use of a system for processing or storing organizational data
- property destruction related to a cybersecurity incident (less than \$100,000)
- personal theft related to a cybersecurity incident (less than \$100,000)
- misuse of organizational property, facilities, and services
- unconfirmed computer virus/worms (depending on impact to business unit and if the infection is the result of a security policy violation)
- undocumented or unapproved vulnerability scans

## **3. LOW-LEVEL CYBERSECURITY INCIDENTS**

Low-level cybersecurity events are the least severe and should be investigated no more than three working days after the incident occurs.

Incidents classified as "Low" include

- loss or compromise of a personal password
- suspected sharing of individually assigned accounts
- minor misuse of organizational property, facilities, and services
- unsuccessful scans/probes (internal and external)
- detected computer virus/worms (depending on impact to business unit)

## Appendix D. Example Incident Reporting Template

### <Organization Name> Incident Reporting Template

Date: \_\_\_\_\_ Name of individual  
Tracking \_\_\_\_\_ completing this form: \_\_\_\_\_  
number: \_\_\_\_\_

#### Incident Priority

<input type="checkbox"/> <b>HIGH</b>	<input type="checkbox"/> <b>MEDIUM</b>	<input type="checkbox"/> <b>LOW</b>	<input type="checkbox"/> <b>OTHER</b>
<i>Additional notes:</i>			

#### Incident Type

*Check all that apply.*

<input type="checkbox"/> Compromised System	<input type="checkbox"/> Lost Equipment/Theft
<input type="checkbox"/> Compromised User Credentials (e.g., lost password)	<input type="checkbox"/> Physical Break-in
<input type="checkbox"/> Network Attack (e.g., DoS)	<input type="checkbox"/> Social Engineering (e.g., Phishing)
<input type="checkbox"/> Malware (e.g., virus, worm, Trojan)	<input type="checkbox"/> Law Enforcement Request
<input type="checkbox"/> Reconnaissance (e.g., scanning, sniffing)	<input type="checkbox"/> Policy Violation (e.g., acceptable use)
<input type="checkbox"/> Unknown/Other (Please describe below.)	
<i>Incident description notes:</i>	

#### Incident Timeline

*Please provide as much detail as possible.*

A. Date and time when the incident was discovered	
B. Date and time when the incident was reported	
C. Date and time when the incident occurred	
<i>Additional timeline details:</i>	

### **Incident Scope**

*Please provide as much detail as possible.*

A. Estimated quantity of systems affected	
B. Estimated quantity of users affected	
C. Third parties involved or affected (e.g., vendors, contractors, partners)	
<i>Additional scoping information:</i>	

### **Systems Affected by the Incident**

*Please provide as much detail as possible.*

A. Attack sources (e.g., IP address, port)	
B. Attack destinations (e.g., IP address, port)	
C. IP addresses of the affected systems	
D. Primary functions of the affected systems (e.g., web server, domain controller)	
E. Operating systems of the affected systems (e.g., version, service pack, patch level, configuration)	
F. Security software loaded on the affected systems (e.g., anti-virus, anti-spyware, firewall, versions, date of latest definitions)	
G. Physical location of the affected systems (e.g., state, city, building, room, desk):	
<i>Additional details:</i>	

### **Users Affected by the Incident**

*Please provide as much detail as possible.*

A. Names and job titles of the affected users:	
B. System access levels or rights of the affected user (e.g., regular user, domain administrator, root)	
<i>Additional user details:</i>	

### **Incident Handling Log**

*Please provide as much detail as possible.*

A. Actions taken to identify the affected resources	
B. Actions taken to remediate the incident	
C. Actions planned to prevent similar incidents	
<i>Additional remediation details:</i>	

### Incident Reporting Information

*Complete this section if incident report was system generated.*

A. Software package	
B. Host ID and location	
<i>Additional system information:</i>	

*Complete this section if an incident report was submitted by an individual.*

A. Full name	
B. Job title	
C. Business unit	
D. Work phone	
E. Mobile phone	
F. Email address	
<i>Additional contact information:</i>	

**Incident Contact Information**

A. Full name	
B. Job title	
C. Business unit	
D. Work phone	
E. Mobile phone	
F. Physical location of affected systems (e.g., state, city, building, room, desk)	

A. Full name	
B. Job title	
C. Business unit	
D. Work phone	
E. Mobile phone	
F. Physical location of affected systems (e.g., state, city, building, room, desk)	

A. Full name	
B. Job title	
C. Business unit	
D. Work phone	
E. Mobile phone	
F. Physical location of affected systems (e.g., state, city, building, room, desk)	

A. Full name	
B. Job title	
C. Business unit	
D. Work phone	
E. Mobile phone	
F. Physical location of affected systems (e.g., state, city, building, room, desk)	

A. Full name	
B. Job title	
C. Business unit	
D. Work phone	
E. Mobile phone	
F. Physical location of affected systems (e.g., state, city, building, room, desk)	

(con't)

A. Full name	
B. Job title	
C. Business unit	
D. Work phone	
E. Mobile phone	
F. Physical location of affected systems (e.g., state, city, building, room, desk)	

A. Full name	
B. Job title	
C. Business unit	
D. Work phone	
E. Mobile phone	
F. Physical location of affected systems (e.g., state, city, building, room, desk)	

A. Full name	
B. Job title	
C. Business unit	
D. Work phone	
E. Mobile phone	
F. Physical location of affected systems (e.g., state, city, building, room, desk)	



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

Table 2 cross-references CRR goal and practice questions for the Incident Management Domain goals, practice questions to the NIST CSF Categories/Subcategories, and the sections of this guide that address those questions. Users of this guide may wish to review the CRR Question Set with Guidance available at <https://www.us-cert.gov/ccubedvp> for more information on interpreting practice questions. The NIST CSF, available at <https://www.us-cert.gov/ccubedvp>, also provides informative references for interpreting Category and Subcategory statements.

*Table 2: Cross-Reference of CRR Goals/Practices and NIST CSF Categories/Subcategories Against the Incident Management Implementation Guide*

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/Subcategory	Incident Management Implementation Guide Reference
Goal 1: A process for identifying, analyzing, responding to, and learning from incidents is established.	—	—
1. Does the organization have a plan for managing incidents? [IMC:SG1.SP1]	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability. PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.	Section III and Appendix A
2. Is the incident management plan reviewed and updated? [IMC:SG1.SP1]	DE.DP-5: Detection processes are continuously improved. PR.IP-10: Response and recovery plans are tested.	Section III, Step 7, Sections VI and V
3. Are the roles and responsibilities in the plan included in job descriptions? [IMC:SG1.SP2]	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability. PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening).	Section III, Step 2
4. Have staff been assigned to the roles and responsibilities detailed in the incident management plan? [IMC:SG1.SP2]	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability. RS.CO-1: Personnel know their roles and order of operations when a response is needed.	Section III, Step 2
Goal 2: A process for detecting, reporting, triaging, and analyzing events is established.	—	—
1. Are events detected and reported? [IMC:SG2.SP1]	DE.CM-1: The network is monitored to detect potential cybersecurity events. DE.CM-2: The physical environment is monitored to detect potential cybersecurity events. DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events. DE.DP-4: Event detection information is communicated to appropriate parties. RS.CO-2: Events are reported consistent with established criteria.	Section III, Step 4 A
2. Is event data logged in an incident knowledge base or similar mechanism? [IMC:SG2.SP2]	DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors.	Section III, Step 4 B

3. Are events categorized? [IMC:SG2.SP4]	RS.AN-4: Incidents are categorized consistent with response plans.	Section III, Step 4 C
4. Are events analyzed to determine if they are related to other events? [IMC:SG2.SP4]	DE.AE-2: Detected events are analyzed to understand attack targets and methods. DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors.	Section III, Step 4 D
5. Are events prioritized? [IMC:SG2.SP4]	DE.AE-4: Impact of events is determined.	Section III, Step 4 E
6. Is the status of events tracked? [IMC:SG2.SP4]	DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors.	Section III, Step 4 F
7. Are events managed to resolution? [IMC:SG2.SP4]	DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors RS.AN-1: Notifications from detection systems are investigated.	Section III, Step 4 G
8. Have requirements (rules, laws, regulations, policies, etc.) for identifying event evidence for forensic purposes been identified? [IMC:SG2.SP3]	DE.DP-2: Detection activities comply with all applicable requirements ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.	Section III, Step 4 H
9. Is there a process to ensure event evidence is handled as required by law or other obligations? [IMC:SG2.SP3]	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed. RS.AN-3: Forensics are performed.	Section III, Step 4 I
Goal 3: Incidents are declared and analyzed.	—	—
1. Are incidents declared? [IMC:SG3.SP1]	RS.CO-2: Events are reported consistent with established criteria.	Section III, Step 5 A
2. Have criteria for the declaration of an incident been established? [IMC:SG3.SP1]	DE.AE-5: Incident alert thresholds are established.	Section III, Step 5 A
3. Are incidents analyzed to determine a response? [IMC:SG3.SP2]	RS.AN-2: The impact of the incident is understood. RS.AN-4: Incidents are categorized consistent with response plans.	Section III, Step 5 D
Goal 4: A process for responding to and recovering from incidents is established.	—	—
1. Are incidents escalated to stakeholders for input and resolution? [IMC:SG4.SP1]	RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams. RS.CO-4: Coordination with stakeholders occurs consistent with response plans.	Section III, Step 6 A
2. Are responses to declared incidents developed and implemented according to predefined procedures? [IMC:SG4.SP2]	RS.MI-1: Incidents are contained. RS.RP-1: Response plan is executed during or after an event.	Section III, Step 6 B
3. Are incident status and response communicated to affected parties? [IMC:SG4.SP3]	RC.CO-1: Public Relations are managed. RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams. RS.CO-3: Information is shared consistent with response plans.	Section III, Steps 3 and 6 B
4. Are incidents tracked to resolution? [IMC:SG4.SP4]	RS.MI-1: Incidents are contained. RS.MI-2: Incidents are mitigated.	Section III, Step 4 C

Goal 5: Post-incident lessons learned are translated into improvement strategies.	—	—
1. Is analysis performed to determine the root causes of incidents? [IMC:SG5.SP1]	DE.DP-5: Detection processes are continuously improved. PR.IP-7: Protection processes are continuously improved.	Section III, Step 7
2. Is there a link between the incident management process and other related processes (problem management, risk management, change management, etc.)? [IMC:SG5.SP2]	DE.DP-5: Detection processes are continuously improved. PR.IP-7: Protection processes are continuously improved.	Sections IV and V
3. Are lessons learned from incident management used to improve asset protection and service continuity strategies? [IMC:SG5.SP3]	DE.DP-5: Detection processes are continuously improved. PR.IP-7: Protection processes are continuously improved. RS.IM-1: Response plans incorporate lessons learned. RS.IM-2: Response strategies are updated.	Sections IV and V

## Endnotes

1. For more information on the *Cyber Resilience Review*, please email the Cyber Security Evaluation Program at [CSE@hq.dhs.gov](mailto:CSE@hq.dhs.gov).
2. The *CERT-RMM* (Glossary of Terms) [Caralli 2010]
3. For more information on the CERT-RMM, please visit <http://www.cert.org/resilience/rmm.html>.
4. The *CERT-RMM* (Glossary of Terms) [Caralli 2010]
5. The *CERT-RMM* (Glossary of Terms) [Caralli 2010]
6. The *CERT-RMM* (IMC: SG1.SP1) [Caralli 2010] describes obtaining commitments to the plan.
7. The *CERT-RMM* (Glossary of Terms) [Caralli 2010]
8. The *CERT-RMM* (IMC: SG2.SP1) [Caralli 2010] describes the process of detecting and reporting events.
9. NIST Special Publication 800-61, *Computer Security Incident Handling Guide* [NIST 2012], discusses how organizations can recognize incidents, including thorough event reporting and analysis.
10. The *CERT-RMM* (IMC: SG2.SP2) [Caralli 2010] discusses why organizations should develop and implement an incident management knowledge base that allows for the entry of event reports (and the tracking of declared incidents) through all phases of the event or incident lifecycle. Guidelines and standards for the consistent documentation of events should be developed and communicated to all who are involved in the reporting and logging processes.
11. NIST Special Publication 800-61, *Computer Security Incident Handling Guide* [NIST 2012], explains log correlation activities and knowledge base concepts.
12. The CERT Division's *Handbook for Computer Security Incident Response Teams (CSIRTs)* [West-Brown 2003] describes how to use logged event data for incident analysis.
13. The *CERT-RMM* (IMC:SG2.SP4) [Caralli 2010] explains that organizations should assign events to a category from the organization's standard category definitions.
14. NIST Special Publication 800-61, *Computer Security Incident Handling Guide* [NIST 2012], explains how events and incidents might be categorized and prioritized and provides some ideas for categories.
15. The CERT Division's *Handbook for Computer Security Incident Response Teams (CSIRTs)* [West-Brown 2003] explains the importance of categorization in incident prioritization.
16. The *CERT-RMM* (IMC: SG2.SP4) [Caralli 2010] discusses the need to perform correlation analysis on event reports to determine if there is affinity between two or more events.
17. NIST Special Publication 800-61, *Computer Security Incident Handling Guide* [NIST 2012], recommends performing event correlation as a validation that events have occurred.
18. The CERT Division's *Handbook for Computer Security Incident Response Teams (CSIRTs)* [West-Brown 2003] explains that the use of event tracking numbers is beneficial to performing event correlation.
19. NIST Special Publication 800-61, *Computer Security Incident Handling Guide* [NIST 2012], discusses prioritization and provides example prioritization factors.

20. The CERT Division's *Handbook for Computer Security Incident Response Teams (CSIRTs)* [West-Brown 2003] explains the importance of assigning a priority to events and incidents.
21. NIST Special Publication 800-61, *Computer Security Incident Handling Guide* [NIST 2012], describes how the status of events may be tracked and suggests that an incident response team should maintain a tracking database to ensure incidents are handled in a timely manner.
22. The *CERT-RMM* (IMC: SG2.SP4) [Caralli 2010] suggests that any event whose status is not "closed" should be assigned a status for further analysis and resolution.
23. The CERT Division's *Handbook for Computer Security Incident Response Teams (CSIRTs)* [West-Brown 2003] provides a case study on how event tracking might be used.
24. The *CERT-RMM* (IMC: SG2.SP3) [Caralli 2010] explains the need to identify relevant rules, laws, regulations, and policies for which incident evidence may be required. Because there may be compliance issues related to the collection and preservation of incident data, this practice must be considered in the context of the organization's compliance program.
25. NIST Special Publication 800-61, *Computer Security Incident Handling Guide* [NIST 2012], explains how laws in evidence collection need to be followed to support law enforcement actions.
26. The CERT Division's *Handbook for Computer Security Incident Response Teams (CSIRTs)* [West-Brown 2003] notes the need to follow laws for forensics operations.
27. The *CERT-RMM* (IMC: SG2.SP3) [Caralli 2010] explains the importance of collecting, documenting, and preserving event evidence. These specific requirements must be included in the organization's logging and tracking process. Some information about events may be confidential or sensitive, so the organization must be careful to appropriately limit access to event information to only those who need to know about it.
28. NIST Special Publication 800-61, *Computer Security Incident Handling Guide* [NIST 2012], explains how laws in evidence collection need to be followed to support law enforcement actions.
29. The CERT Division's *Handbook for Computer Security Incident Response Teams (CSIRTs)* [West-Brown 2003] notes the need to follow laws in order to support forensics operations.
30. The *CERT-RMM* (IMC:SG3.SP1) [Caralli 2010] discusses incident declaration criteria and provides some examples.
31. NIST Special Publication 800-61, *Computer Security Incident Handling Guide* [NIST 2012], explains how incident analysis supports response prioritization.
32. The CERT Division's *Handbook for Computer Security Incident Response Teams (CSIRTs)* [West-Brown 2003] explains how incident declaration criteria support incident analysis.
33. The Department of Energy's *Cyber Security Incident Management Manual* [U.S. Department of Energy 2009] provides an example of incident declaration criteria for use by the U.S. Department of Energy.
34. The *CERT-RMM* (IMC: SG3.SP2) [Caralli 2010] details incident analysis activities.
35. NIST Special Publication 800-61, *Computer Security Incident Handling Guide* [NIST 2012], examines incident analysis and recommends actions that support it.
36. The CERT Division's *Handbook for Computer Security Incident Response Teams (CSIRTs)* [West-Brown 2003] details incident analysis concepts.

37. The *CERT-RMM* (IMC: SG4.SP1) [Caralli 2010] explains the need for incident escalation procedures, including escalation criteria.
38. The *CERT-RMM* (IMC: SG4.SP1) [Caralli 2010] describes options for response.
39. NIST Special Publication 800-61, *Computer Security Incident Handling Guide* [NIST 2012], details incident notification, including typical stakeholders and communication channels.
40. The CERT Division's *Handbook for Computer Security Incident Response Teams (CSIRTs)* [West-Brown 2003] discusses escalation criteria, information to be included in incident communication, and considerations when escalating multiple events.
41. The *CERT-RMM* (IMC: SG4.SP2) [Caralli 2010] addresses the need to develop an incident response strategy and plan to limit incident effect and repair incident damage.
42. The *CERT-RMM* (IMC: SG4.SP3) [Caralli 2010] outlines concepts important to an organizational incident management communications plan.
43. The *CERT-RMM* (IMC: SG4.SP4) [Caralli 2010] identifies the importance of tracking incidents to closure and recording the closed state of incidents.
44. NIST Special Publication 800-61, *Computer Security Incident Handling Guide* [NIST 2012], discusses how organizations can use collected incident data to support lessons-learned activities and identify systemic weaknesses in its system of internal controls.
45. See *Jane's Crisis Communication Handbook* [Fernandez and Merzer 2004].
46. The *CERT-RMM* (IMC: SG4.SP3) [Caralli 2010] outlines concepts important to an organizational incident management communications plan.
47. NIST Special Publication 800-61, *Computer Security Incident Handling Guide* [NIST 2012], addresses components of incident communications plans and identifies typical stakeholders that require notification.
48. The CERT Division's *Handbook for Computer Security Incident Response Teams (CSIRTs)* [West-Brown 2003] discusses escalation criteria, information to be included in incident communication, and considerations when escalating multiple events.
49. The *CERT-RMM* (IMC: SG5.SP1) [Caralli 2010] describes practices in performing root-cause analysis of cybersecurity incidents.
50. NIST Special Publication 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations* [NIST 2010], identifies minimum requirements for lessons-learned activities.
51. The *CERT-RMM* (IMC: SG5.SP2) [Caralli 2010] suggests that incident documentation should be used in the organization's overall problem management processes and that problem management can identify opportunities to improve how procedures are executed.
52. NIST Special Publication 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations* [NIST 2010], outlines attributes of incident data that are used to gain an organization-wide perspective on incidents.
53. The *CERT-RMM* (IMC:SG5.SP3) [Caralli 2010] suggests that organizations review incident knowledge base information.

54. NIST Special Publication 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations* [NIST 2010], discusses the need to use incident information to ensure the continuation of the organization's missions and services.
55. The CERT Division's *Handbook for Computer Security Incident Response Teams (CSIRTs)* [West-Brown 2003] discusses how documented incidents can support the organization's risk management efforts.
56. FEMA's *National Incident Management System* provides additional information about planning, available at <http://www.fema.gov/national-incident-management-system>.
57. The CERT Division's *Handbook for Computer Security Incident Response Teams (CSIRTs)* [West-Brown 2003] describes the construction of incident response plans and teams and explains the incident management lifecycle.
58. NIST Special Publication 800-61, *Computer Security Incident Handling Guide*, Sections 2.3 and 2.4, at <http://www.csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf>, describes plan creation and plan components.
59. The CERT Division's *Handbook for Computer Security Incident Response Teams (CSIRTs)* [West-Brown 2003] addresses the establishment and assignment of responsibilities as a part of establishing organizational guidelines for CSIRTs.
60. NIST Special Publication 800-61, *Computer Security Incident Handling Guide* [NIST 2012], addresses the assignment of staff to teams.
61. NIST SP 800-84, *Guide to Test, Training and Exercise Programs for IT Plans and Capabilities*, at <http://www.csrc.nist.gov/publications/nistpubs/800-84/SP800-84.pdf>, provides testing guidance.
62. *Tabletop Exercises for Incident Response Plans Under NERC Reliability Standard CIP-800*, at <http://ics-cert.us-cert.gov/sites/default/files/ICSJWG-Archive/F2010/Simon%20-%20Tabletop%20Exercise%20Webinar.pdf>, addresses the preparation, scenario creation, execution, evaluation, and results recording for incident response exercises.
63. NIST Special Publication 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations* [NIST 2010], addresses the revision of the incident response plan to address system or organizational changes or problems encountered during plan implementation, execution, or testing.
64. The CERT Division's *Handbook for Computer Security Incident Response Teams (CSIRTs)* [West-Brown 2003] explains the need to validate the incident management policy as well as the importance of maintaining the policy as the organization changes.
65. See the USDA Computer Incident Response Procedures Manual DM 505-000.